# Network-Centric Warfare: Implications for Operational Design

**A Monograph**
**by**
**LTC Jeffrey R. Witsken**
**United States Army**


**School of Advanced Military Studies**
**United States Army Command and General Staff College**
**Fort Leavenworth, Kansas**
**First Term AY 01-02**

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

LTC Jeffrey R. Witsken

Title of Monograph: Network Centric Warfare: Implications for Operational Design

Approved by:

| | |
|---|---|
| _____ | Monograph Director |
| Peter J. Schifferle, Ph.D. | |
| _____ | Professor and Director Academic Affairs, School of Advanced Military Studies |
| Robert H. Berlin, Ph.D. | |
| _____ | Director, Graduate Degree Program |
| Philip J. Brookes, Ph.D. | |

# Abstract

NETWORK CENTRIC WARFARE: IMPLICATIONS FOR OPERATIONAL DESIGN by LTC Jeffrey R. Witsken, US Army, 62 pages.

The United States military is adapting itself to fight warfare in the Information Age, preparing forces that use information superiority as a key weapon. Advocates of this communication-based and information-based form of warfare use the term "Network-Centric Warfare" to describe the new paradigm. This new form of warfighting is expected to fully exploit the power of shared information and superior communications. Both of the recent "Joint Vision" documents, Joint Vision 2010 and Joint Vision 2020, embrace this new form of warfare as a central feature of the future of the US military. But does Network-Centric Warfare significantly alter operational design of a campaign?

Network-Centric Warfare is essentially warfare that generates combat power by effectively linking (networking) actors, sensors, and decision-makers. Shimon Naveh's definition of a campaign (as the competition of two competing complex systems) helps frame the context and relevance of Network-Centric Warfare. Given this context, one cannot underestimate the central importance of the sensor network to the overall effectiveness of the networked force. A campaign planner must consider the abilities and limitations of his sensor network as he plans the campaign, and design appropriate actions accordingly. Additionally, the campaign planner must carefully balance dispersion and mass to counter erosion of forces and sustain operational momentum. A campaign plan must contain the right balance of Network-Centric Warfare and traditional means to attain operational objectives.

Since Operation Desert Storm, the joint services have gradually achieved partial networking, which exhibits many of the anticipated features of Network-Centric Warfare. Communications and information system capabilities are enabling geographically dispersed operations, collaboration among key agencies and leaders, and reachback to distant resources. Joint forces now employ adaptive and persistent sensor networks, although limitations persist in what these sensors can realistically achieve. The sensor network is highly integrated with fires, and is regarded as an integral enabler of effects and maneuver. Ground units are gaining the ability to dominate expanded battlespace, and integrate fully into the networked force. Finally, network-centric capabilities are increasing the operational reach and synergy of each service's forces. Network-Centric Warfare is now a key element of modern campaign design.

Network-centric operations permit the use of widely dispersed forces across an expanded battlespace, but there is a balance needed between dispersion and mass needed for operational momentum. Sensor networks are now essential for network-centric campaign success. A planner must consider operational reach in at least three key areas: sensors, fires, and physical occupation of terrain. His planning needs to provide operational pressure at decisive points, by concentrating superior force (sensors, fires, maneuver forces). In summary, Network-Centric Warfare has dramatically affected operational design. Operational reach and lines of operation have gained additional complexity. Sensor network employment must be considered a key element of operational design, and an integral feature of operational maneuver. By improving the relationships between joint forces in the US operational system, Network-Centric Warfare promises to yield a decisive advantage.

# Table of Contents

## Figures

CHAPTER ONE

# Introduction

Improvements in communication and information technologies over the last 10 years hint at potential for powerful new military capabilities. Recognizing this, the United States military is adapting to fight warfare in this "Information Age", and has published two vision statements: Joint Vision 2010 and Joint Vision 2020. These vision statements point to a future force using information superiority as one of its key weapons. In pursuit of this vision, the Department of Defense is heavily investing in advanced communications and information systems. As these systems become available, all the services are developing concepts, changing doctrine, and adapting organizations to fully leverage their potential.[1]

Deeply embedded within the Joint Vision documents is recognition that information technology will enable a new form of warfighting. Advocates of this information-based and communication-based form of warfare use the term "Network-Centric Warfare" to describe the new paradigm. This new form of warfighting is expected to fully exploit the power of shared information and superior communications. Technological advances in sensor and communication technology suggest that tightly integrated systems of sensors and weapons could dramatically alter the abilities of all four services. Both of the recent "Joint Vision" documents, Joint Vision 2010 and Joint Vision 2020, embrace this new form of warfare as a central feature of the future of the US military. But beyond the broad concepts expressed in these documents, what can we really expect from "Network-Centric Warfare", and does it significantly alter operational design of a campaign? This monograph is specifically intended to help answer that question.

[1] Although Network-Centric Warfare is deeply embedded within Joint Vision documents, it is generally not found in current doctrinal publications by that name. Instead, its concepts are being incorporated within the emerging concepts of each service. These concepts envision aggressive leveraging of Network-Centric Warfare to gain significant advantage over future enemies.

Given the promise of expanded capabilities of joint forces enabled by Network-Centric Warfare, it is appropriate to assess what changes are occurring that are relevant to operational planning. Doctrine stresses that a coherent operational design properly utilizes available resources to attain campaign aims. Therefore, successful operational planning requires both a proper understanding of force capabilities and of the conditions required for success. Planners must understand the capabilities and limitations of Network-Centric Warfare. For these reasons, this monograph will explore how Network-Centric Warfare appears to be changing the military services (with an emphasis on the US Army), and what impact of these observed trends have regards campaign planning and operational design.[2]

Campaign planning utilizes all the appropriate elements of US military force to provide the most problems for the enemy. Joint doctrine stresses synergy between forces, which is reinforced when operations are integrated and extended through the depth of the theater. Joint doctrine stresses the integrated nature of campaigns:

> Campaigns are joint. They serve as the focus for the conduct of war and often in operations other than war. A wartime campaign is the synchronization of air, land, sea, space, and special operations—as well as interagency and multinational operations—in harmony with diplomatic, economic, and informational efforts to attain national and multinational objectives.[3]

Elements of the joint force conduct operations that synergistically reinforce the other elements. Air, sea, space and special operations facilitate land operations, while land operations protect bases, and enable air, sea, space and special operations throughout the theater.[4]

---

[2] Current Army doctrine does not specifically recognize the term "Network-Centric Warfare". However, later discussion will show that network-centric concepts are deeply embedded in Army operational and organizational concepts.

[3] Joint Chiefs of Staff, *Joint Publication 3-0: Doctrine for Joint Operations.* Washington, D. C., 1995, III-5.

[4] See Joint Chiefs of Staff, *Joint Publication 3-0: Doctrine for Joint Operations.* Washington, D. C., 1995, III-5, and Joint Chiefs of Staff, *Joint Publication 1: Joint Warfare of the Armed Forces of the United States*. Washington, D. C., 1995, IV-2.

The synergy noted in joint doctrine can only be achieved when commanders and their planners seek the proper combination of forces, aiming to achieve campaign objectives with minimal cost in casualties and time. This synergy depends greatly on shared understanding of the operational situation within the command.[5]

Since the primary question concerns operational design, a brief doctrinal definition is appropriate. According to Joint Publication 1-02, operational design is the set of key considerations used as a framework in the course of planning for a campaign or major operation. It is primarily a means for commanders to visualize the operation, and shape their intent. FM 3-0 identifies several elements of operational design, and discusses each in detail. A proper operational design has the proper selection, integration, and synchronization of forces and resources to achieve campaign aims. [6]

## Methodology

The monograph begins by reviewing joint doctrine and Army doctrine, with emphasis on defining the elements of operational design, and the role of operational maneuver. The next step is a review of joint vision documents, identifying service concepts incorporating Network-Centric Warfare. This review includes emerging US Army operational and organizational concepts to identify those changes the Army envisions. The next step is to define Network-Centric Warfare, and apply within the context of Shimon Naveh's operational theory. Naveh's theory forms a framework, which lends context to operational level expectations for this new "warfare".

Expectations are followed by an examination of selected experiments, military operations, and studies. This charts the extent and form of Network-Centric Warfare's emergence. The analysis

[5] JCS, *Joint Publication 3-0*, III-9 to III-11.
[6] Joint Chiefs of Staff, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, Washington, D. C., 2002, 319. Also see HQDA, *FM 3-0*, 5-6 to 5-12. This section fully explains each element of operational design, which are identified as endstate/military conditions, center of gravity, decisive points/objectives, lines of operation, culminating point, operational

will assess what capabilities are being realized, and what trends are present in US military operations. The conclusion is an assessment of the observed results and trends against each of the monograph's criteria.

This monograph's delimitation must be understood. First, there is a clear emphasis on the role of ground forces within a "network-centric" campaign design. Hence, there are fundamental presuppositions that political will exists to allow the employment of ground forces, and that certain campaign objectives cannot be achieved without employment of ground forces. Furthermore, this monograph partially addresses the challenges of coalition warfare, and the challenges of conducting a campaign with legacy and transformation forces.[7]

Also included is a partial examination of sister service concepts, given the monograph's focus is on ground forces. The monograph confines itself to campaigns against enemies that offer the opportunity to practice operational art, that present a "palpable medium" for the application of operational design. Hence, the monograph primarily addresses campaigns against organized military forces, employed in an "operational" fashion, pursuing their own campaign objectives. [8]

## Criteria

The paper's criteria are specifically intended to help answer the question, "Does Network-Centric Warfare alter operational design of a campaign?" Each criterion will be assessed using

---

reach/approach/pauses, simultaneous/sequential operations, linear/nonlinear operations, and tempo.

[7] A planner must be skillful in the developing the correct blend of forces within his campaign. The force pool he can draw from will undoubtedly be a complex mixture of legacy, interim, and objective forces. The challenge will be to apply available forces within the campaign in a way that optimizes the strengths of each type of force, while producing an overall blend that achieves campaign objectives. Undoubtedly, the planner must establish conditions that permit these forces to interface with each other, avoiding serious gaps in operational tempo. This requires specific attention to communications planning, permitting the entire force to work effectively in spite of vast differences in communications and information capability among units.

[8] The concepts and implications expressed in this monograph may in fact be applicable to stability and support operations, or to campaigns against enemies that are not operationally inclined. Recent operations in Bosnia, Kosovo, and Afghanistan suggest that this is so. However, the monograph focuses on operationally-minded opposing sides to attain the maximum possible clarity regards the implications. See James J Schneider, *The Structure of Strategic Revolution* (Novato, CA: Presidio Press, 1994), 50-53.

the elements of operational design. The first criterion asks what precursors or aspects of Network-Centric Warfare are occurring? The second criterion assesses sufficiency of internetted

sensors and precision fires to achieve campaign objectives. The third criterion assesses any changes in the employment of joint forces within a campaign, by identifying increased capabilities and potential changes in service roles. The fourth criterion asks if Network Centric Warfare may have changed the nature of operational maneuver within a campaign.

CHAPTER TWO

# Joint and Service Vision

Network-centric concepts are deeply embedded within Joint Vision 2010 and Joint Vision 2020, and each of the respective service visions. Since most joint doctrine was written before the release of the Joint Vision documents, there is limited mention of network-centric concepts, so joint doctrine is not heavily addressed here.[9] This chapter summarizes key aspects of the joint service visions, to include reviewing US Army Operational and Organizational Concepts (O&Os).

Network Centric Warfare is described as a means to achieve Joint Vision 2020, by creating an asymmetric information advantage. The Department of Defense is pursuing initiatives intended to provide the foundation for Network-Centric Warfare, guided by the Joint Vision. Critical automated C4I systems are being fielded, and continually improved. Clearly there is a deep commitment by the Department of Defense and each of the services to implement Network-Centric Warfare. [10]

The United States Air Force is pursuing implementation of a global capability for network-centric warfare. The Air Force is integrating new command and control tools and sensor systems, which promise improved collaboration and interoperability. With these systems, the Air Force is better able to deploy into theater, plan missions, and conduct operations effectively. Improvements over the next decade will strive to establish a system for adaptive execution of

[9] For example, the Joint Doctrine Encyclopedia addresses "network", identifying the impact of networks on military operations, and stressing that Joint Forces will have to adapt to these emerging environments. See Joint Chiefs of Staff, *Joint Doctrine Encyclopedia,* Washington, D. C., 1997, 550.

[10] Department of Defense, Assistant Secretary of Defense for Command, Control, Communications, & Intelligence. *Network Centric Warfare: Department of Defense Report to Congress (27 July 2001)*, 2-4. Also See Appendix A of this report for a detailed discussion of each service's integration of Network-Centric Warfare into its overall service vision. Available at http://www.c3i.osd.mil/Network-Centric Warfare/. Site last visited 20 March 2002. Also see The Joint Staff, C4 Systems Directorate, Information Superiority Division (J6Q), *Enabling the Joint Vision*, Washington, D. C., May 2000, 1-4. Available at http://www.dtic.mil/jcs/j6/enablingjv.pdf. Site last visited 20 March 2002.

decisions within minutes. New sensors capabilities are planned to support expansive reconnaissance and strike capabilities, and to provide useful means of striking fleeting targets.[11]

Both the US Navy and the USMC are working diligently to implement Network-Centric Warfare within their operations. The US Navy is perhaps the most aggressive service in moving towards a network-centric capability. The Navy's concept reaches beyond its traditional roles of sea control. Developments under way improve the Navy's ability to project power ashore, and provide supporting fires inland, often hundreds of miles. The US Marine Corps is leveraging the Navy's work, and implementing its own programs to improve its operational capabilities. The "Ship to Operational Maneuver" concept calls for Marine forces to be capable of conducting strikes and operational maneuver hundred of miles inland past the coastline.[12]

The Army, for its part, is digitizing its existing force, and developing both Interim and Objective Forces that fundamentally rely on network centric operations. The Army is also fielding command and control systems and advanced sensor platforms, which will facilitate network-centric operations.[13] Over the last two years, elements of TRADOC have updated the Force XXI Organizational and Operational Concept (O&O), while writing the Interim Force O&O, and the emerging Objective Force O&O. Each concept envisions units that are expected to dominate geographic areas much larger than current units. These concepts indicate that maneuver forces will use internetted sensors and fires as part of highly dispersed operations.

---

[11] See DOD, ASD C3I, *Network Centric Warfare: Department of Defense Report to Congress*, B-19 to B-25. Also see David A Deptula, "Embracing Change: US Air Force Transformation Will Expand the Nation's Strategic Options", *Armed Forces Journal International*, October 2001, 69-71.

[12] See DOD, ASD C3I, *Network Centric Warfare: Department of Defense Report to Congress*, B-9 to B-19. Also see Scott Redd, "Sustained Assured Access: The Navy's Role in Joint Warfare", *Armed Forces Journal International*, September 2001, 66-70. Also see James Lasswell, "Waterborne Warriors: Putting The Amphibious Pieces Together", *Armed Forces Journal International*, January 2001, 36-41.

[13] DOD, ASD C3I, *Network Centric Warfare: Department of Defense Report to Congress*, B-1 to B-8.

## Army Organizational and Operational Concepts

The Army's Force XXI concept was the initial effort to leverage network-centric concepts within its forces, by integrating modern command and control technology with the latest sensors and weapon platforms. The fruit of this initiative is an integrated force, using information dominance to overmatch enemy forces. The Force XXI Organizational and Operational Concept (O&O) envisions leveraging of information to dramatically increase the size of the battlespace assigned to Force XXI division and brigades. The division is expected to dominate a battlespace of 120x240 kilometers. Brigade battlespace is defined as 2700 square kilometers with its organic units, and one-third of the division's battlespace (8000 square kilometers) when augmented. [14]

The Interim Force is fundamentally network-centric in its character. The Interim Brigade O&O explicitly incorporates internetted combined arms capabilities. In addition, the Brigade is equipped with large numbers of advanced sensors (on air and ground platforms). The Interim Brigade is intended to execute distributed and dispersed operations over an expanded battlespace, operating over a 50x50 kilometer area (2500 square kilometers). If augmented properly, the Brigade is expected to be capable of operating across a 100x100 kilometer battlespace (10,000 square kilometers). This combination of advanced command and control, extensive sensor suites, and situation awareness enables a new way of warfighting:

> Organic C4ISR capabilities and high mobility enable the IBCT to operate according to a new tactical paradigm. In the past, maneuver forces normally: 1) made contact with the enemy; 2) developed the situation further while in contact; 3) then conducted maneuver for decisive action. Owing to enhanced SU, the IBCT will often be able to: 1) develop the situation out of contact; 2) maneuver rapidly to positions of advantage; 3) and then initiate contact at the time and place of the commander's choice to achieve decision.[15]

---

[14] Headquarters, United States Army Training and Doctrine Command. *Operational and Organizational (O&O) Concept for the Army XXI Division-level Heavy Force, Including the Brigade Combat Team and the Cavalry Squadron (Coordinating Draft)*, Fort Monroe, VA, December 1999, 13-18 and 20-21.
[15] Headquarters, United States Army Training and Doctrine Command. *The Brigade Combat Team Organizational and Operational Concept, Final Version*, Fort Monroe, VA, 30 June 2000, Chapter 1, page 8.

The Interim Force therefore assumes sufficient situation awareness to move away from the old paradigm of physically deploying maneuver units across the battlespace to gain situation awareness. That information will now come from the sensor network. [16]

The emerging Objective Force Concept incorporates tenets of Network-Centric Warfare to an even greater degree than the Interim Force. Echoing FM 3-0, the Objective Force is intended to "see first, understand first, act first, and finish decisively." The Objective Force leverages a "Tactical Infosphere", which enables access to situation awareness and targeting resources. Objective Force units are expected to dominate additional battlespace over the interim force, given their ability to fully exploit relevant information, employ enhanced organic fires, and leverage joint fires. One early conceptual briefing postulates a battalion-size unit could potentially use its fires to dominate some 2800 square kilometers, with the ability to employ supporting fires over a 9500 square kilometer area. Although these figures are conceptual, the point is that an Objective Force battalion-size unit may potentially dominate the battlespace of a Force XXI or Interim Brigade.[17]

[16] Ibid., Chapter 3, page 33.

[17] Headquarters, United States Army Training and Doctrine Command, *Draft TRADOC Pamphlet 525-3-91, Objective Force Maneuver Unit of Action Concept*, Fort Monroe , VA, September 2001, 15-16. Estimates of area dominated assumes complete sensor coverage of the area, that the Unit of Action is occupying a 5km radius area (78km$^{2)}$, that it has a 12km Line of Sight (LOS) fires and Beyond Line of Sight (BLOS) fires range (907 km$^{2)}$, and a 25km Non Line of Sight (NLOS) range (2826 km$^{2)}$, and access to supporting fires out to a 50km radius (9499 km$^{2)}$. See Headquarters, United States Army Training and Doctrine Command, *The Objective Force Maneuver Unit of Action Concept Briefing*, Fort Monroe , VA, 24 January 01.

CHAPTER THREE

# What is Network-Centric Warfare?

Current literature provides multiple interpretations of Network-Centric Warfare. This chapter advances a description of Network-Centric Warfare, and applies it to operational theory to establish a framework for evaluating its value within a campaign.

Network-Centric Warfare is described as the result of advances in sensor technology, information technology, weapon technology, and the synergies produced by these technologies working together. It generates combat power by effectively linking (networking) actors, sensors, and decision-makers. This permits military operations to occur with greater speed and precision, creating operations that optimize combat efficiency. By improving a force's communication and decision processes, units are able to generate combat power quickly and better synchronize their efforts with the larger force.[18]

The following figures may be useful to illustrate the concept of Network-Centric Warfare. A given force can be considered to possess a certain mixture of sensors and weaponry, which allow it to observe and project lethal force to some distance beyond the area it physically occupies. [19] In general terms, a force exerts a great deal of control in the areas it physically occupies, and exerts lesser degrees of control into areas where it can only observe or direct fires.

Consider a non-networked force with limited information flow between units and platforms. Each individual platform must rely on its own sensors, as it does not receive much external information, and can only provide limited information to the larger force. As a result, a force

[18] Edward A. Smith, Jr., "Network-Centric Warfare: What's the Point?" *Naval War College Review*, Winter 2001, 60-62. Available at http://www.nwc.navy.mil/press/Review/2001/Winter/art4-w01.htm. Site last visited 15 January 2002.

[19] Throughout this monograph, the term "sensors" refers to the full range of assets available to a military force, which allow it to observe and orient itself to its environment and the enemy force. This includes not only mechanical sensors (such as vehicle sights, radar, UAVs, and satellites), but also all forms of human intelligence (HUMINT: scouts, special forces, and agents) available to the force.

wishing to dominate a large area must deploy sufficient quantities of sensors and weapons platforms to ensure coverage for situation awareness purposes. Units must continually employ screening forces and reserves to guard against unexpected, undetected enemy activity. As the enemy is located, the non-networked force must mass combat power (fires and ground combat systems) to obtain desired results against enemy units. Such massing is usually achieved by the physical concentration of systems, so that all involved can coherently act against the enemy. Since situation awareness is limited, and localized, significant numbers of massed formations are needed to provide sufficient combat power wherever it may be needed.

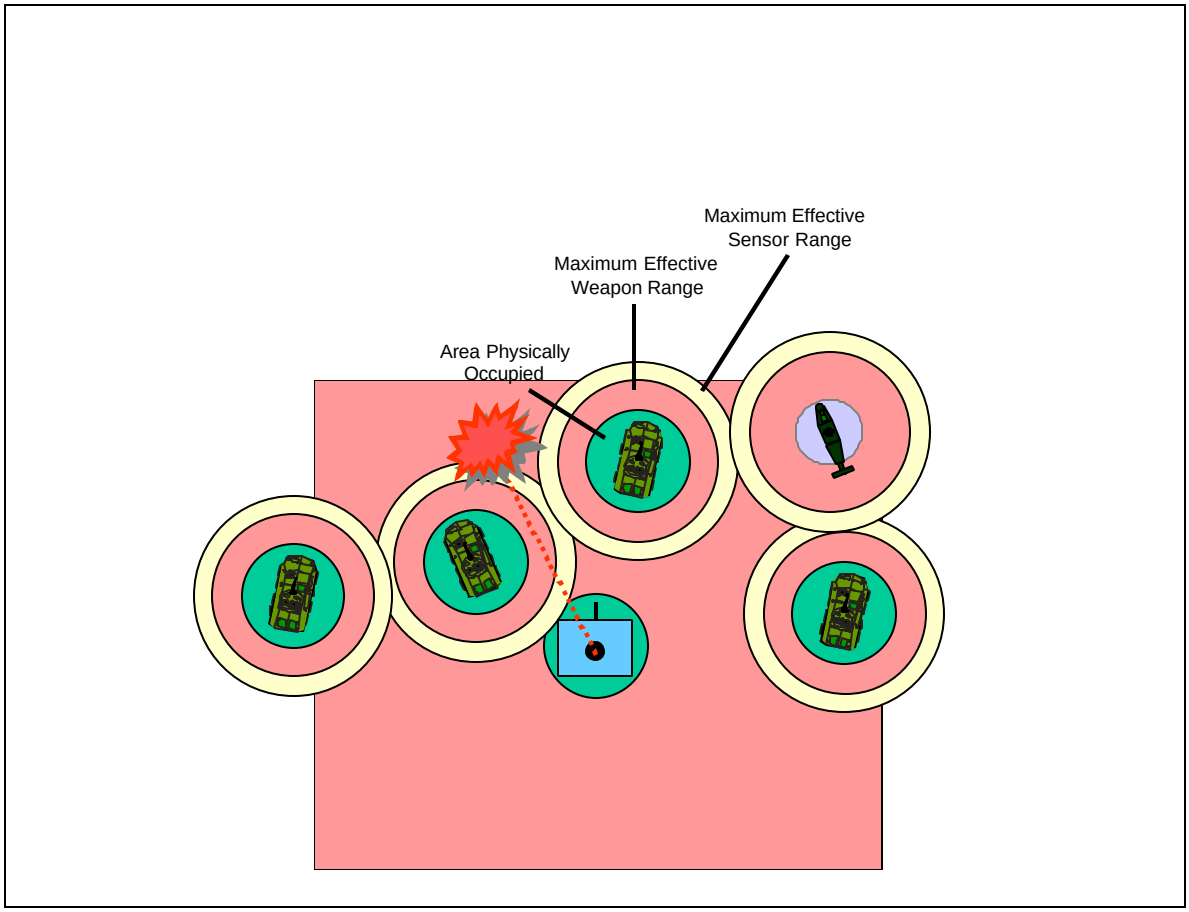


**Figure 1. Traditional Non-Networked Force**

When a unit is effectively networked several distinct changes occur. The first change is improved situation awareness. Each unit now receives information from all available sensors. Commanders are freed from dissipating combat forces throughout the battlespace solely for

situation awareness and security purposes (the sensor network effectively performs this function). All weapons can potentially attack any location within range, so combat power can be applied effectively against the enemy from dispersed locations. Commanders have less need to generate large, massed formations intended to overwhelm any enemy detected. Instead, application of fires and massed ground combat forces can be focused at critical locations.[20] Please note that the requirement to mass fires and forces has not been eliminated, but instead becomes more precise in execution.

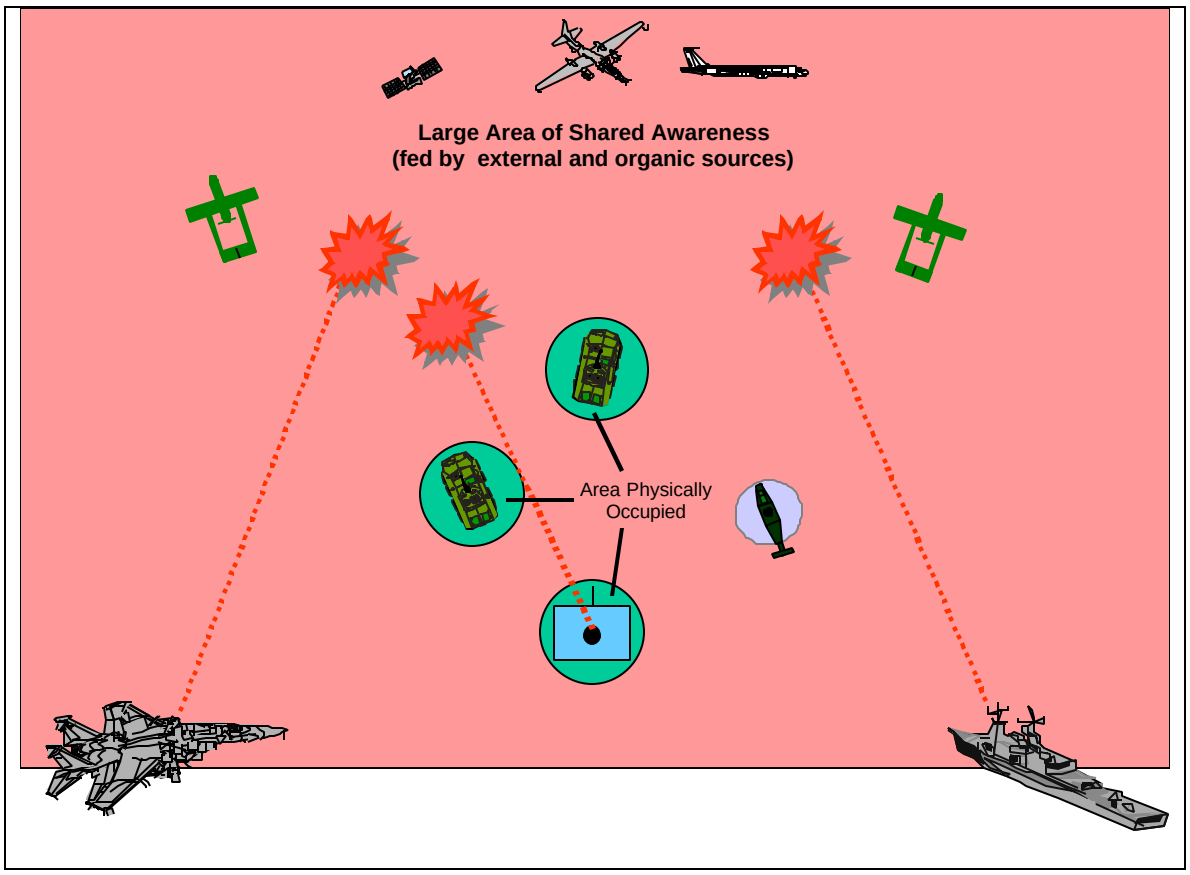


**Figure 2. Networked Force**

Therefore, Network-Centric Warfare can be defined as geographically dispersed forces, sharing a high quality situation awareness, that are collaborating and synchronizing as needed to achieve the commander's intent. Despite an unprecedented degree of dispersion, Network-

[20] Paul Murdock, "Principles of War on the Network Centric Battlefield: Mass and Economy of Force",

Centric Warfare allows forces to act in a cohesive, integrated fashion. It effectively connects the various elements of operational forces, with impacts at the tactical, operational, and strategic levels. The various sensors employed become effectively networked, thus providing shared situation awareness throughout the friendly force. Decision-makers are effectively linked, to the point that they can effectively collaborate and interact while remaining geographically dispersed. This networking of actors within the battlespace is expected to permit highly precise, high tempo operations, outstripping the enemy in space and time.[21]

Network-Centric Warfare splits sensors, decision-makers, and weapons platforms, yet permits all to work as one. This splitting from the old model of unitary platforms generates unique considerations. Recall the sensor area, weapon area, and area of physical control model discussed earlier in this chapter. The sensor network is the portion of the network-centric force that builds situation awareness and enables the effective utilization of fires and maneuver by dispersed friendly forces. Shared awareness allows a relatively efficient combination of fires and ground forces to attack elements of the enemy operational system. As Robert Leonhard noted, "we achieve economy by focusing not on a weapon's lethality, but rather on its complementary effects on other friendly weapons."[22] In this sense, the sensor network is what enables lethality, and permits the network-centric force to function at all.

Network-Centric Warfare depends heavily on a sensor network, which is employed independent of weapons platforms, yet is linked to the appropriate intelligence and targeting agencies (as well as the entire force for situation awareness purposes). This network provides the information for decisions at all levels, and allows tactical units to effectively act on the

---

*Parameters*, Vol. XXXII, No 1. Spring 2002, 87-90.

[21] Alberts, David S., John J. Garstka, Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority, 2d Edition Revised* (Washington, DC: CCRP Publications, 2000), 88.

[22] Robert R. Leonhard, *The Principles of War for the Information Age*, (Novato, CA, Presidio Press 1998), 221.

battlefield. These situationally aware small units understand their situation in relation to the enemy and terrain. They collaborate, and are capable of "self-synchronization". Self-synchronization is characterized as:

> …This type of highly decentralized C2 calls for lower-level decision–makers to be guided only by their training, their understanding of their commander's intent, and their awareness of the situation in relevant portions of the battlespace.[23]

Besides self-synchronization, the benefits of fully networked forces include improved decision-making, lethality, survivability (due to an improved ability to manage risk), and responsiveness. Also, responsive and efficient logistical support will yield a faster tempo to operations. Finally, units are expected to occupy and control an expanded area.[24]

The prerequisites for a network-centric force are a capable sensor network, robust communications, the ability to generate and share high quality situation awareness, and the ability to collaborate regarding this awareness.[25] These prerequisites are not easily achieved, requiring considerable investments in technology and proliferation of these capabilities throughout the force by continuous modernization. So Network-Centric Warfare does not just "show up," but emerges as investments are made in these key areas.

## Naveh's Operational Theory

It is insufficient to apply network-centric concepts to the operational design elements listed in FM 3-0. For a more effective analysis, an operational theory needs to be applied to provide effective context. Shimon Naveh's system theory of operational art is useful for analysis in this monograph. He drew heavily from the general system theory of Bertalanffy, who postulates that

---

[23] Quote is from Alberts, David S., John J. Garstka, Richard E. Hayes, David A. Signori, *Understanding Information Age Warfare*. (Washington, DC: CCRP Publications, 2001), 219. Also see related discussion on pages 26-29.

[24] Alberts, et. Al., *Network Centric Warfare*, 65-68 and 140-141. Also see Department of Defense, Assistant Secretary of Defense for Command, Control, Communications, & Intelligence. *Network Centric Warfare. Department of Defense Report to Congress*, (Washington, DC: CCRP Publications, 27 July 2001), 3-11.

contending militaries can be seen as complex, open systems ("open" refers to the fact that these systems interact with their environment). Each of these systems is composed of three elements: the number of entities in the system, the type or attributes of the entities in the system, and the relationships between the entities in the system. Each system has an aim that gives it a unifying purpose, with each entity possessing a specific task or goal related to the unifying aim.[26]

An important consideration is a campaign's physical framework in time and space. Naveh illustrated the Russian operational idea of that a campaign consists of acts of warfare, directed to achieve a mission, within a given space and timeframe. Essentially, a campaign tries to achieve an aim, using a framework of individual fights or battles, within a given physical space and timeframe. The operational level contains a "cognitive tension" between tactical objectives and the overall larger aim.[27]

Naveh defined a campaign as competition of two competing complex systems, operating within the time and space of the theater. These systems compete with each other, trying to attain "operational shock" against the other system, or in other words, prevent it from functioning. Ways to achieve operational shock are to separate the command from the system, divide or fragment the system, force it into a situation where it cannot achieve its aim or maintain its equilibrium, or attack its centers of gravity.[28]

Naveh contends that operational art contains a balance of holding and striking forces, of attrition and maneuver forces. In essence, operational fires wear down the enemy system, and help create opportunities for decisive maneuver. Fires are not separate from operational maneuver, but an integral part of it. Operational maneuver considers the whole problem

---

[25] Ibid., 3-7 to 3-11.
[26] Shimon Naveh, *In Pursuit of Military Excellence: The Evolution of Operational Theory* (Portland, OR: Frank Cass Publishers, 1997), 4-9 citing Ludwig Von Bertalanffy, *General System Theory*, New York, 1975.
[27] Ibid., 7, 9-12.
[28] Ibid., 15-18.

holistically: "a simultaneous combination of various forms of combat in a unified maneuver."[29] In a similar vein, attrition is not of itself decisive, as the enemy system can still function and adapt. Only maneuver can finally halt the functioning of the enemy system decisively. An operational system also requires the right balance of quantity and quality, as a limited quantity of high quality forces can be quickly eroded away by enemy action and the physical demands of a theater (time and space factors).[30]

Another key concept for Naveh is mass, which is the key for sustaining operational momentum within a campaign. Naveh points out that operational forces are subject to "erosion". Operational forces lose strength over time due to enemy action, movement over great distances, physical exhaustion, disease, mechanical breakdown, lack of supplies, and other factors related to the friction of war. Mass overcomes this erosion by providing sufficient forces and sustainment to enable friendly forces to overcome enemy action, distance, and other factors to sustain action against the enemy operational system. Hence, mass enables operational momentum. Analysis later in this monograph will use Naveh's system approach (competing systems, operational shock, attrition vs. maneuver, mass vs. erosion (momentum), and operational maneuver) to address the impacts of Network-Centric Warfare. [31]

## Application to Operational Theory

By robustly networking the elements of a force, Network-Centric Warfare improves the ability of that force to achieve campaign aims. First of all, networking changes and/or improves the relationships among the elements of the friendly complex system.[32] By "greasing the skids" of

[29] Ibid., 185.
[30] Ibid., 7, 22-23.
[31] Ibid., 145, 185. Naveh's concept of mass generally applies to the physical aspects of mass. There are also moral or cybernetic aspects of inducing operational shock, which Network-Centric Warfare includes.
[32] Network-Centric Warfare also incorporates elements of advances in sensor and weapons technologies, which change the type and attributes of entities in the friendly operational system. See Smith, "Network-Centric Warfare: What's the Point?" 59-64.

the friendly operational systems, it enables the overall operational system to maintain equilibrium and overcome the friction of the campaign environment. It also improves the friendly force's ability to attack and frustrate the enemy system, thus placing the enemy's system in operational shock.

Assuming an effective sensor network, a networked force can effectively attrit the enemy force, and maneuver in an efficient, precise way against the enemy. Network-centric capabilities ease the challenges of a campaign's physical framework in time and space. A networked force can readily achieve mass (via effects and/or via physical concentration) from highly dispersed locations. This improved ability to mass maintains momentum and counters the impact of time and space factors (and the resulting "erosive effects" on forces due to increased dispersion). In summation, the networked force is far better equipped to conduct the "holistic, integrated operational maneuver" described by Naveh.

## The Network-Centric Campaign

If Network-Centric Warfare delivers as advertised, it seems that campaign planning needs to fully consider the capabilities of networked forces, and utilize a very different operational design (compared to non-networked forces). Operational art must still be applied, specifically in terms of correctly assessing the enemy's operational system (and discerning its centers of gravity and vulnerabilities). But the campaign must then be fashioned to employ the force to achieve operational shock of the enemy system. To do this properly, the astute campaign planner must consider the essential functioning of a network-centric force.

A planner must realize the central importance of the sensor network to the overall effectiveness of the networked force. A campaign planner should plan to employ a sensor network that reveals the essential portions of the operational system. He must anticipate elements of the enemy operational system that are indiscernible (due to concealment, enemy action, or lack

of sensor capability.) To maximize success, a varied mixture of sensors, able to capture multiple attributes of the enemy's activity, will be most successful in identifying his actions and enable destruction (by trying to avoid one type of sensor, the enemy is detectable by other types).[33]

Naveh's contention that operational art contains a balance of attrition and maneuver forces, and quantity and quality remains a valid consideration.[34] To achieve such a balance, a campaign plan must employ sensor networks to detect elements of the enemy's operational system (or centers of gravity). But then the question is whether which elements of the enemy systems are susceptible to attack by attrition (through lethal and non-lethal means). But a networked force cannot effectively attack elements that cannot be detected by the sensor network. When the sensor network is limited or insufficient, a network-centric force must maneuver forces to gain observation of the enemy system, or must establish physical control of geographic areas to prevent functioning of the enemy system.

Finally, the campaign planner must carefully consider the erosive effects of the enemy force and the theater itself (time and space). He must allow for sufficient forces to counteract these erosive effects, concurrently frustrating the enemy's "mass," and maintain operational momentum toward the campaign objectives.[35] Hence, a campaign plan must contain the right balance of networked and traditional means to attain operational objectives. A campaign planner must correctly identify this balance, and employ his forces (as part of operational maneuver) against the enemy's operational system.

---

[33] Leonhard, *The Principles of War for the Information Age*, 71-74.

[34] Naveh, *In Pursuit of Military Excellence*, 22-23. Naveh does not account for information operations and non-lethal means of attack. Planners must address these tools as part of their plans to frustrate the enemy system.

[35] A planner has to assume that the enemy will be striving to upset the friendly operational system, and to achieve their own campaign aims. Therefore, the enemy can be expected to mass both to counter friendly maneuver, and to establish momentum toward their campaign goals.

CHAPTER FOUR

# The Emergence of Network-Centric Warfare

Only six years have passed since Joint Vision 2010 was published, hence the US military is still early in the acquisition and fielding of systems designed to fulfill the current Joint Vision. In order to find evidence of the progress made thus far, it is necessary to review significant experiments, military operations, and studies. Thus our review will look for the emergence and impact of partial networking of US military forces (key agencies, platforms, sensors, and decision-makers). Since Operation Desert Storm predates discussion of the Network-Centric Warfare concept (which first emerged in the 1995-1996 timeframe), it provides an effective baseline for evaluation of later trends. This review is intended to indicate which Network-Centric Warfare capabilities actually exist, and are relevant to future US military operations. This chapter thus represents the application of our first criterion to the monograph's central question.

## 1991: Operation Desert Storm

At the time of Operation Desert Storm, the US military had only begun to implement information age technologies. Communications capability within the theater was severely limited, forcing a reliance on civilian communication networks. Communications between services, even between the most capable sensor and command and control systems (such as AWACS and Aegis ships) was limited, and unreliable. Within the Army, tactical communications were predominantly AM and FM radio, which limited information dissemination to voice transmissions and facsimile. The limited range of these communications made for a spotty communication network within the theater. Use of special microwave communications provided a limited e-mail capability, again with some reliability issues. Given the demands of a mobile campaign, this communication

network frequently broke down, and precluded short notice synchronization of operations, except when voice communications were established.[36]

Operation Desert Storm contained a few examples of sensors that provided information to multiple commanders simultaneously. The Air Force conducted reconnaissance with satellites and manned reconnaissance aircraft, and employed its AWACS aircraft to maintain awareness of air operations. Ground units received intelligence updates from USMC Pioneer Unmanned Aerial Vehicles (UAVs) and British drone aircraft to gain intelligence of Iraqi defensive positions. JSTARS was rushed into employment, feeding information from its sensors to both air and ground commanders. Relayed from special ground stations, such information frequently made it to Corps commanders to inform their decisions, and occasionally was pushed to the regiments and brigades. Operation Desert Storm saw limited linkage of sensors to weapons platforms, including counterbattery radar, the use of JSTARS to direct air strikes, and the use of UAVs to direct shore bombardment by battleships. [37]

In Operation Desert Storm, the few sensors feeding commanders provided partial information. Satellites provided some information regarding the theater, but not on a timely basis, and not in readily digestible form. Aircraft sensors could not provide sufficient detail regarding bombing assessments. JSTARS provided useful information concerning enemy activity, but could not provide sufficient detail to reveal Iraqi intent. However, there was very little fusion that occurred with available sensor inputs, except what a given commander could accomplish given the information he was privy to at the moment.[38]

---

[36] Gordon, Michael R., Bernard E. Trainor, *The General's War: The Inside Story of the Conflict in the Gulf* (New York: Little, Brown, and Co., 1995), 64, 264, 387-389.
[37] Stephen A. Borque, "Desert Saber: The VII Corps in the Gulf War" (Ph. D. diss., Georgia State University, 1996), 195-196. Also see James Blackwell, *Thunder in the Desert,* (New York: Bantam Books, 1991), 120. Also see U. S. News and World Report, *Triumph without Victory* (New York: Random House, 1992), 347.
[38] U. S. News and World Report, *Triumph without Victory,* 275-277. Also see Gordon and Trainor, *The General's War,* 384, 406, 436.

Given communication limitations and the limited ability to share information, the employment of ground forces in Operation Desert Storm continued in "traditional" forms. Without a useful "near-real time" sensor network, and given limited information from intelligence sources, the burden of attaining local situation awareness fell on the ground combat formations. This requirement helped lead to a nearly continuous front of friendly units intended to determine the surface and composition in depth of the Iraqi defenses.

The fact that the Iraqis were deployed in organized defensive formations necessitated the need for coalition ground forces to physically mass. Division frontages ranged from 25-45 km, and the depth of each division's area varied from 80-150km. Within this battlespace, the combat power of each division was concentrated forward, arrayed in wedge or column formations to permit the physical massing of hundreds of weapons systems at critical points and provide momentum. The reason for this massing was to provide combat power, which would overcome successive, integrated Iraqi defensive positions. Brigade frontages shrank to as little as six kilometers, in order to gain such mass. As the operation unfolded, the depth in formations, and physical massing of systems provided the combat power and momentum to fight through the Iraqi defensive system.[39]

Operation Desert Storm was a campaign with a limited sensor network, a partial ability to fuse information and a minimal ability to disseminate that information. Because of these conditions, commanders had to employ ground formations to gain situation awareness, and had to physically mass forces over large frontages to overwhelm the enemy's "massed" forces. For our purposes,

[39] Borque, "Desert Saber", 305, 311. Additional information can be gleaned from the operational sketches included within the VII Corps After Action Reports. Combined Arms Research Library, Gulf War Collection, Group VII Corps, SG Historian, SSG AAR1-009, Part 1 (Executive Summary and Historical Narrative). Also see Richard M. Swain, *"Lucky War": Third Army in Desert Storm*, (Fort Leavenworth, KS: U. S. Army Command and General Staff College Press, 1994), 244.

Operation Desert Storm becomes a baseline, from which we will chart the emergence of Network-Centric Warfare.

### 1995-1998: Operations Deliberate Force & Joint Endeavor

Operation Deliberate Force was an air and sea operation conducted in August and September 1995 to support peace efforts in the Balkans. Deliberate Force involved the coordination of forces from several NATO nations, spread across bases in Albania, Italy, Germany, France, and on ships in the Adriatic Sea. Advanced command, control, and communications tools supported planning and coordination, including frequent consultations among commanders and political leaders. Operation Deliberate Force witnessed UAVs playing a larger reconnaissance and surveillance role. In a few cases, certain sensors were linked with analysts to develop assessments of for targeting and damage assessment purposes. [40]

Beginning in December of 1995, a sustained peacekeeping operation (Operation Joint Endeavor) began in Bosnia. As the mission progressed, technology advances served to better integrate the widely dispersed peacekeepers (known as the Implementation Force or IFOR). A web-based data network and secure VTC capability enabled frequent collaboration and coordination among the IFOR components and supporting agencies. Employed in even larger numbers, UAVs provided sustained intelligence gathering, in some cases providing near real time video to command centers. Additionally, support from a multitude of space-based, aerial, and ground-based sensors, were integrated by theater-level analysis centers. Each US service component established their own common tactical picture for monitoring operations. Taken together, these improvements enabled effective command and control despite significant dispersion among all the elements of IFOR.[41]

---

[40] Owen, Robert C., *Deliberate Force: A Case Study in Effective Air Campaigning*, (Maxwell AFB, AL: Air University Press, 2000), 54, 160-163, 180-182.

[41] Ibid., 111, 137, 227-228. Also see Wentz, Larry K., *Lessons From Bosnia: The IFOR Experience*,

## 1998-1999: Operation Allied Force

During late 1998 and early 1999, Operation Allied Force attempted to create conditions for peace in Kosovo. Much larger than Operation Deliberate Force, Operation Allied Force eventually encompassed air, sea, and land operations, all benefiting from further technological advancement in C4I technology. Improvements in communications generated improvements in intelligence fusion and targeting of time-sensitive targets, permitting a process which integrated intelligence analysts, planners, and decision-makers in Italy, Belgium, England, and the United States to identify and decide targets. In essence, the location of an individual, or a staff agency, did not prevent their contribution to the targeting process. This approach permitted raw intelligence to be quickly analyzed and fed into the targeting process, producing improvements in the attack of fleeting targets. This "reach-back" capability enabled forces forward deployed to leverage resources outside of their theater. As such, Operation Allied Force demonstrated an improved ability to develop high quality situation awareness and share it as needed. [42]

Operation Allied Force represents the first employment of an adaptive, collaborating sensor network. Available sensors were partially networked to each other, and to intelligence and operations centers. This networking continued to mature as the operation continued. JSTARS was utilized again, this time in conjunction with Army and Air Force UAVs (UAV employment reached the highest levels experienced to date). Eventually, JSTARS was employed as a cue to these UAVs, as well as attack aircraft. Predator UAV imagery was routed through satellite communications to the Combined Air Operations Center, where targeting decisions were made and based to airborne command and control aircraft. Hunter UAV video was relayed through to

---

(Washington D. C.: Institute for National Strategic Studies, 1998), 67-68, 355-358.

[42] Michael Ignatieff, *Virtual War: Kosovo and Beyond,* (New York: Metropolitan Books, Henry Holt and Co., 2000), 99-101. Also see Ivo Daalder and Michael O'Hanlon, *Winning Ugly: NATO's War to Save Kosovo*, (Washington, D. C.: Brookings Institution, 2000), 236.

provide near real time video to decision-makers. Navy F-14s and FA18s beamed imagery and video to operations centers, using strap-on surveillance pods.[43]

TF Hawk (the ground element of Allied Force) became a key element of the sensor network during this campaign. Although originally intended to strike targets deep within Kosovo with attack helicopters, TF Hawk (EH-60s, Hunter UAVs, and RC-12 Guardrail) was valued more for its ISR capabilities than its offensive capability (the planned attacks were never authorized). Although TF Hawk physically occupied a small sector within Albania, its sensors reached far into Kosovo, hence contributing significantly to the overall effort. TF Hawk ended up influencing a significant area of terrain, far beyond the area it physically occupied and controlled. [44]

Despite improvements in overall sensor network integration and performance, challenges persisted during Operation Allied Force. JSTARS and UAVS were not able to provide the targeting information needed against Serbian forces, due to sensor limitations. The collection effort was further hindered by Serbian proficiency in camouflage, dispersal, and decoys, weather, and terrain conditions. The Serbians actively attacked UAVs, shooting down many.[45]

Operation Allied Force represents further advances in collaboration and information dissemination capabilities. Additionally, an increased number and variety of sensor platforms were integrated into an overall network of increasing capability and duration. This network was partially linked to fires, enabling fairly rapid targeting in some cases. Operation Allied Force also illustrated a growing capability to employ weapons systems from dispersed locations (including the continental United States) to support operational fires. Another innovation is the use of ground forces as an additional ISR resource. In the future, "battlefield calculus" involves not only the

---

[43] Ivo Daalder and Michael O'Hanlon, *Winning Ugly: NATO's War to Save Kosovo,* (Washington, D. C.: Brookings Institution, 2000), 236. Benjamin S. Lambeth, *NATO'S Air War for Kosovo: A Strategic and Operational Assessment*. (Santa Monica, CA: Rand, 2001), 94, 96, 124, and 126-127. Also see Alberts, Garstka, Hayes, and Signori, *Understanding Information Age Warfare,* 277-279.
[44] Lambeth, *NATO'S Air War for Kosovo,* 127 and 157.

weapons assigned, but also sensor capability, which will enable application of organic and supporting combat power.

## 2001: The Division Capstone Exercise

Prior to 2001, there was limited experience regarding networked ground forces, with the exception of Operation Joint Endeavor (a peacekeeping operation). Questions remained regarding the utility of advanced information technology and sensors in a medium to high intensity combat environment. In 2001, the Division Capstone Exercise (DCX) was conducted to demonstrate the extant capabilities of the Army's first "digital" division. Although a training exercise, DCX stressed the division's ability to function across an expanded battlespace under severe environmental conditions. The units participating in DCX boasted a full suite of C4I systems and data communications to the platoon and individual vehicle level. These Force XXI organizations featured a higher ratio of ISR assets to maneuver formations, and digital links to supporting fires. Until a fully digitized ground force is employed in combat, DCX is our best source of information regarding the capabilities of ground forces in a networked environment. [46]

In Phase I, the brigade combat team was able to successfully meld information from external and organic sensors to gain situation awareness, build a common tactical picture, and successfully disseminate that information vertically and laterally. This information flow was sufficient to allow

---

[45] Ibid., 96-97, 123-124, 126.

[46] DCX consisted of two phases. Phase I featured maneuver and live fire training of a digitized brigade combat team at the National Training Center. Since the NTC was not large enough to provide the full battlespace suggested by the Force XXI O&O, a wrap-around simulation environment was built around the physical training area to permit operations across the full O&O battlespace. Phase II, a Battle Command Training Program exercise, occurred in October 2001 at Fort Hood, Texas. This phase was conducted entirely using simulation. Additional ISR assets included the Tactical UAV and a Brigade Reconnaissance Troop organic to the maneuver brigades, supported by division UAV assets and external sensors such as JSTARS. Supporting fires included cannon artillery, rocket artillery, and close air support with a situation awareness data link (SADL). See TRADOC Analysis Center, *Final Report for the Division Capstone Exercise (DCX*), *TRAC-F-TR-02-006*, Fort Leavenworth, Kansas, March 2002, 1. Additional ISR assets included the Tactical UAV and a Brigade Reconnaissance Troop organic to the maneuver brigades, supported by division UAV assets and external sensors such as JSTARS. Supporting fires included cannon artillery, rocket artillery, and close air support with a situation awareness data link (SADL).

a degree of self-synchronization to occur within the brigade. During Phase II, the BLUFOR was able to provide its tactical information to higher echelons, demonstrating the ability to participate in a joint Common Operational Picture. The brigade leveraged external sensors and organic ISR assets to successfully employ artillery and close air support at extended ranges to damage enemy forces. During Phase II, ISR systems generated the vast majority of fire missions, and the division readily employed organic and supporting fires.[47]

The DCX experience suggests the digital brigade and division were potentially capable of fighting within their prescribed battlespace. The brigade and division achieved an effective balance between massed and dispersed combat power. Both fires and maneuver forces were massed as needed to counter the enemy's mass wherever encountered. The brigade and division could also maneuver dispersed forces to deal with enemy flanking attacks and rear area security operations. Situation awareness specifically enabled movement of dispersed forces (usually the reserve task force) to critical locations. If DCX can be considered an indication that the Force XXI battlespace is achievable, then a four-fold increase in battlespace over Operation Desert Storm can be realized.[48]

---

[47] The BLUFOR effectively exploited JSTARS and UAVs to attain unprecedented levels of lethality with CAS and artillery fires. In several battles, CAS was the second most lethal BLUFOR system. In another battle, use of the TUAV enabled highly lethal counterbattery fires, destroying over 75% of OPFOR artillery. The extended situation awareness provided by these sensors allowed the Brigade to fight well beyond close combat distances. See TRAC, *Final Report for the Division Capstone Exercise (DCX)*, C-5 to C-7, C-13 to C-14, C-83 to C-85, C-91 to C-93, C-97 to C-100. *Also see* TRADOC Analysis Center, *Initial Insights Memorandum (IIM) for the Division Capstone Exercise Phase II (DCXII), TRAC-F-TR-02-004*, Fort Leavenworth, Kansas, October 2001, 22-23, 26.

[48] In terms of physical dispersion, the digital brigade operated within sectors of up to 1750 square kilometers. This area was constrained by the physical terrain limitations of the NTC training area, and cannot be considered indicative of battlefield conditions. Yet if you consider the additional area covered by brigade sensors and fires, (which includes areas of the simulation wrap-around environment) you easily reach a 2700 square kilometer area. Unit battlespace described in the Force XXI O&O (a division area of up to 28,800 square kilometers) is compared to unit battlespace during Operation Desert Storm (division areas ranging from 2000-6750 square kilometers). This increase in dispersion was possible largely due to the supporting communications network (the Tactical Internet). Despite some materiel limitations, units could operate beyond FM communication range, yet still effectively communicate with data communications across extended distances. See TRAC, *Final Report for the Division Capstone Exercise (DCX)*, C-3 to C-10, C-91 to C-93.

The quality of situation awareness helped compensate for a scarcity of ground combat power, and reinforced the need for an effective sensor network to permit the effective generation of combat power. Large areas of terrain where effectively unoccupied, as the BLUFOR specifically massed only where circumstances dictated that massing of forces and fires was needed to get the job done.[49]

The significant point of DCX is that the US Army is making progress in fielding networked formations at the brigade and division level. Although still undergoing refinement, these formations are leveraging network-centric concepts within the ground combat environment. This increased capability has operational implications. First, ground forces can apply a degree of operational pressure simply by establishing sensor coverage of their expanded battlespace. Secondly, the ability of these formations to leverage network-centric concepts allows the force to efficiently apply its mass and maintain operational momentum. These advances may reduce the overall requirement for forces within a campaign.[50]

## 2001-Present: Operation Enduring Freedom

Operation Enduring Freedom indicates further progression toward Network-Centric Warfare. Although there is limited information available currently about operations in Afghanistan, there is clear evidence that network-centric capabilities are permitting an unprecedented level of cooperation among deployed forces. Operation Enduring Freedom is seeing increased dissemination of information (including a true joint common operational picture). Ground forces are equipped with terminals that permit access to intelligence networks, and with position location

[49] During DCX Phase I, it was noted that the sensors available could not provide all information required, and the Exercise reinforced the need to integrate all available sensor systems (air and ground) to gain the necessary level of situation awareness, without relying on a few select systems. TRAC, *Final Report for the Division Capstone Exercise (DCX)*, C-8 to C-10, C-24 to C-27

[50] The quantity, size, and type of units utilized within a campaign represents a complex decision by the operational commander. This issue will be discussed in more detail in Chapter Five.

devices that automatically report the location of equipment and personnel. Moreover, information dissemination is improving as well between ground elements and supporting aerial platforms.[51]

Recent events in Operation Enduring Freedom suggest that US forces have achieved a highly adaptive sensor network in Afghanistan. There has been increased use of UAVs and other sensor platforms to provide long loiter sensor capability (including P3 Orion aircraft and the new Global Hawk UAV system). This network features teaming of sensors and sensor platforms to cue each other, permitting "persistent ISR": a system of sensors that, as a group, maintains continuous observation of a given area.[52]

Thus far, Operation Enduring Freedom indicates that commanders are recognizing that proper employment of sensor systems is a critical precondition to employing fires and gaining situation awareness. The employment of ISR systems is seen as the first part of mission and receives as much attention as weapon platform employment. Increased communications capability is being shared between UAVs, JSTARS, and AC-130 gunships, and there is increased use of the latest data link (Link-16) among sensors and weapons systems. For example, streaming video can now be passed from UAVs to attack aircraft. Aggressive actions are underway to expand this initial capability, permitting additional dissemination of information within the theater. Close air and ground force cooperation was also apparent, as Special Forces located targets that were undetectable from the air, and close air support aircraft struck them.[53]

---

[51] Stan Crock, "Cooperation: A Key to Victory in Afghanistan", *Business Week Online*, December 17, 2001. Available at http://www.businessweek.com/bwdaily/dnflash/dec2001/nf20011217_5178.htm. Site last visited 20 March 2002. Also see Vernon Loeb and Thomas E. Ricks., "1's and 0's Replacing Bullets in U. S. Arsenal.", *Washington Post*, February 2, 2002. See also Jeremy Singer and Frank Tiboni, "New Intel Devices Get Trial By Fire in Afghanistan," *Defense News*, March 25-31, 2002, 8.

[52] David A. Fulghum, "Navy Exploits P-3 in Overland Recce Role", Aviation Week & Space Technology, March 4, 2002. Also see Frank Tiboni, "Instantaneous Attack Capability Near for US", *Defense News*, January 7-13, 2002.

[53] Fulghum, "Intel Emerging As Key Weapon In Afghanistan", Aviation Week & Space Technology, March 11, 2002. Also see Frank Tiboni, "Instantaneous Attack Capability Near for US." Also see Elaine M. Grossman, "Air Force Chief Launches Major Effort to Improve Targeting", *Inside the Pentagon*, November 8, 2001. Also see Burger, Kim and Andrew Koch, "Afghanistan: The Key Lessons", *Jane's Defence Weekly*,

Operation Enduring Freedom is already remarkable as a campaign that utilizes ground forces, in a highly precise and focused manner, across an expanded battlespace. For example, Army and Marine operations initially concentrated vicinity of Bagram and Kandahar (where USMC forces were projected over 400nm from the sea). These operations seized key airfields, and then used them as operating bases for later operations.[54] Logistical support has been provided over extended distances, from many existing US bases outside of Afghanistan. This support relies heavily on the "reachback" concept to accomplish equipment and personnel support. This dispersed, long-range employment of ground forces is prosecuting operations with a minimal footprint of soldiers in country.

Operation Anaconda, conducted from 2-18 March 2002, is illustrative of the challenges surrounding operations with dispersed forces. During this operation, Afghan and US ground forces attacked a concentration of enemy forces in Paktia province (detected by the sensor network discussed above). Although initially dispersed at Bagram and Kandahar, ground forces using transport helicopters concentrated in the vicinity of the enemy force to trap it. Close air support (USAF and USN aircraft operating from Diego Garcia, aircraft carriers, and other bases in the region) and attack helicopters concentrated to support the ground effort.[55]

Apparently, the ISR network had not detected the full strength and disposition of the enemy forces. The initial days of fighting were more severe than anticipated, due to the unexpectedly fierce resistance. Although friendly forces retained the initiative, it currently appears that insufficient mass was present (relative to the enemy force and terrain) to quickly overwhelm the

---

January 2, 2002.

[54] John Diamond, "Pentagon Plumbs Lessons From the War", *Chicago Tribune*, January 14, 2002.

[55] Thomas E. Ricks and Bradley Graham, "Surprises, Adjustments, and Milestones for U. S. Military," *Washington Post*, March 10, 2002.

enemy force. As a result, the tactical operation took longer to achieve than initially planned, and additional forces were subsequently deployed into the theater to sustain operational momentum.[56]

Enduring Freedom features precise use of military forces tailored to threat and terrain. Although dispersed, they are working to a common end. The supporting sensor network is continually focused and reinforced to provide the needed degree of situation awareness. Ground elements augment the sensor network when needed attain the required picture, and to permit the direction of fires. Operational maneuver by dispersed forces is possible across great distances (as long as adequate bases and lift platforms are available). Given the level of implementation of network-centric concepts, historians may declare Operation Enduring Freedom as the first network-centric military operation.

## A Look Ahead: The TRADOC Combined Arms Reconnaissance Study

A recent study (the TRADOC Combined Arms Recon Study) addressed the future environment as fielded information and sensor technologies continue to improve. Entirely simulation-based, this study examined the impact when robust, high capacity C4I systems fully networked a reconnaissance force and maneuver forces. The study found that a networked force specifically maneuvers sensors and reconnaissance platforms as a precondition for effectively employing combat power. Shared awareness enabled immediate fires from organic and external assets, to the point where the reconnaissance and sensor platforms directed most fires.[57]

The Study further suggested that reconnaissance forces can develop a high level of situation awareness, enabling maneuver forces to remain out of contact until necessary, leading to mission accomplishment in shorter time and with fewer losses. Given information from the entire suite of

[56] Ibid.

[57] Occasionally this meant conducting offensive operations to enable sensor employment to generate the needed level of information, which in turn would further enable maneuver by ground forces. See TRADOC Analysis Center, *TRADOC Combined Arms Reconnaissance Study Phase II (TRAC-L-TR-01-005)*, Fort Leavenworth, KS, 15 December 2000, 81, 94-101, 118-127, 153-161, 237-242..

relevant sensors, maneuver forces could focus organic reconnaissance assets, and forsake physically maneuvering across the entire battlespace. Instead, forces maneuvered to "blend" sensor capabilities in certain areas. For example, ground reconnaissance platforms were employed specifically in areas where aerial platforms or external sensors could not provide the needed level of awareness.[58]

The Combined Arms Recon Study indicates that a robustly networked force recognizes its dependence on the sensor network, and specifically employs this network as part of the scheme of maneuver. Judicious sensor employment permits precise maneuver, resulting in less erosion of ground forces, enabling them to have additional impact on the battlefield (tactically and operationally).

## Assessment: The Current State of Network-Centric Warfare

Based on this historical review, it is now time to form the answer to the first monograph criteria. What aspects of Network-Centric Warfare are actually here today? Chapter Three identified five characteristics of a network-centric force. These characteristics are dispersed forces within an expanded battlespace, a sensor network, shared high quality situation awareness, ability for decision makers to collaborate from remote locations, and self-synchronization. This historical review indicates that the DOD investment is paying off, and Network-Centric Warfare is emerging as a key element of modern campaign design. However, its emergence is gradual. We are in fact currently experiencing is a partially networked force.

What has happened as result of this partial investment in Network-Centric Operations? As seen in operations since 1995, there is a clear trend toward dispersed, yet focused use of forces within a campaign. Another trend is the emergence of a sensor network, tied closely to fires. Operation Enduring Freedom further highlights the importance of this sensor network to

[58] Ibid., 109-116, 129-135, 149-151.

operational fires and maneuver. The quality of situation awareness continues to improve, from humble beginnings in 1995 to the current day, with a joint common operational picture. The ability of decision-makers to collaborate from remote locations continues to improve, having reached the point where headquarters do not need to deploy into theater. Only self-synchronization is not prevalent (currently only noted within the DCX exercise). This is undoubtedly due to the limited degree of digitization across the joint force at this point in time.

In Naveh's terms, Network-Centric Warfare is altering the US joint operational system (types of entities, their attributes, and their relationships). It is enabling the use of a complex, dispersed, yet unified framework of battles to attack enemy operational systems. It is permitting the efficient generation and use of combat power, thus creating mass (powerful in terms of its efficiency, precision, and focus) to sustain operational momentum. The answer to the first criterion is that Network-Centric Warfare exists today, albeit in partial implementation. Since the U. S. military is partially "network-centric", and partially "traditional", the considerations for campaign planning are clearly complex. It is crucial to understand the implications for operational design.

CHAPTER FIVE

# Network-Centric Warfare and Campaign Planning

The US military today is a partially networked force, which is becoming more networked daily as force modernization and transformation continues. Evidence suggests that all of the features expected of Network-Centric Warfare are occurring to a degree, making the impacts identified at the conclusion of Chapter 3 relevant for consideration.[59] Partial networking certainly affects the joint force, in terms of the relationships among the elements of the friendly operational system. This partial networking also improves the friendly force's ability to attack and frustrate the enemy system. Part of the challenge for the campaign planner is assessing how the extent of networking changes the character of his own forces. For example, he must estimate how effective a sensor network he can employ, and gauge its impact on friendly and enemy systems. He must assess how dispersed his force can be, yet still achieve requisite mass (via effects and/or via physical concentration).

## The Sufficiency of Sensors and Fires to Accomplish Campaign Aims

The second criterion asks if a sensor network and linked fires are adequate to accomplish campaign aims. Today's sensor networks feature extensive cross-cueing and cooperation between sensors and effects platforms. The result is the emergence of sensor networks of increasing performance (in terms of detection capability, area observed, and duration), and the "persistent ISR" concept. Each service is working to further improve individual sensor capabilities, and fielding additional platforms. A planner must learn how to leverage these networks for both tactical and operational effect.

The performance of sensor networks has improved to the point that these networks are critical enablers for situation awareness (which enables fires and maneuver). Operation Enduring

Freedom indicates that sensor networks are being considered in this light. In today's environment, combat power and operational reach depend on the ability to extend and maintain situation awareness. As such, commanders are learning to maneuver sensor networks with the same intensity as traditional combat forces.

This review reveals both the promise of sensor networks and their persistent limitations. Despite advances, all of the historical cases reviewed highlight that sensors have their limitations and weaknesses. Network-Centric Warfare relies heavily on effective sensors. In a general sense, a network-centric force can only respond to stimuli the sensor network detects. Furthermore, sensors have varying qualities, endurance, strengths, and weaknesses. They can be blinded, destroyed, confounded, and deceived. Recognizing this, modern armies place a premium on conducting complex operations making maximum use of cover, concealment, and dispersion. [60] The experience of the last ten years indicates that despite tremendous advances, we have yet to attain a sensor and precision fires network that will identify and attack all aspects of an enemy system. Operation Allied Force contains examples of fulfilled campaign aims (attack of Serbian infrastructure) and unfulfilled aims (destruction of the Serbian forces within Kosovo).

The answer to this criterion (are sensors and fires sufficient to attain campaign aims) depends heavily on a planner's initial campaign analysis. If a campaign aim involves attack of detectable enemy operational systems, then sensors and fires will suffice quite well (although there is the caution that fires, as an element of attrition, can only slow an enemy system, and not destroy it). Experience indicates that current joint forces can readily attack those portions of the enemy's operational system that are detectable. The key question is what decisive enemy points and operational systems are visible to the sensor network? The challenge is that many enemy systems

---

[59] See pages 17-19 above.

[60] Stephen Biddle, Wade P. Hinkle, and Michael P. Fischerkeller, "Skill and Technology in Modern War", *Joint Forces Quarterly*, Summer 1999, 23-24.

are partially detectable, or undetectable. Sensor networks and operational fires fail in these cases. The wise planner knows the difference.

A campaign planner will make provisions for establishing a sensor network as part of the campaign. The campaign's structure would place sensor networks at the proper time and space to detect elements of the enemy system, enabling attack by fires and/or by physical control. But he must consciously avoid the "sensors can see it all" trap. He must be sensitive to the limitations of the planned sensor network relative to the enemy's operational system. This is particularly true when the enemy has discovered how to operate outside of sensor capabilities, or has effective countermeasures. In these cases, other methods are required to attack the enemy operational system.

When sensors and fires cannot adequately achieve campaign aims, the planner should consider other tools, and he should do so within the framework of operational maneuver. Naveh stated that operational maneuver considers the problem holistically: "a simultaneous combination of various forms of combat in a unified maneuver."[61] Recognizing the limitations of fires, a planner must turn to maneuver to gain the means to achieve his aims.

Operational maneuver offers the solution to these situations. Recent experience suggests that there are now three potential means within operational maneuver to attain campaign aims. First of all, maneuver offers to place forces in position to gain observation of previously undetectable portions of the enemy's operational system, thus enabling operational fires (TF Hawk as an example). Secondly, maneuver can place forces to physically attack the enemy system. Thirdly, maneuver can prevent the enemy system from functioning by gaining and controlling key terrain. Operational maneuver can employ any combination of these three methods (as well as fires) to attain desired objectives.

[61] Naveh, 21.

## Implications Regards Joint Force Employment

The third criterion asks what implications exist for joint force employment. Even in today's partially networked environment, there are clear implications for force employment. For example, this historical review indicates that information technology improvements are permitting a great degree of dispersion across the theater. Today's standard is dispersed forces operating within the depth of the theater (as seen in Operations Allied Force and Enduring Freedom). Reachback enables a campaign planner to leverage assets worldwide. This capability can significantly reduce deployment requirements, since many agencies and units can perform their functions from home station or intermediate locations. This reduces the need to place units in theater, which can limit deployment and logistical challenges within the theater. The campaign planner must grasp what these capabilities are, so he can structure the theater without involving extraneous forces.

### The Role of Sensor Networks

Entities within a complex operational system can be considered to possess a certain mixture of sensors and weaponry as attributes which allow them to observe and project lethal force to some distance beyond the area they physically occupy. In general terms, a force exerts a great deal of control in the areas it physically occupies, and exerts lesser degrees of control into areas where it can only observe or direct fires. A networked force splits sensors, decision-makers, and weapons platforms, yet permits all to work as one (effectively changing the types of entities, their attributes, and their relationships with each other). This is a key difference from the traditional model of unitary platforms (which combined sensors, weapons, and decision-makers within a single platform). The new, network-centric operational system generates unique considerations.

Network-Centric Warfare heavily relies on sensor networks for situation awareness, which enables effective warfighting. Recognizing this, every military operation in the last ten years has utilized the best possible sensor network possible. Recent experience indicates that sensor

networks are primary enablers of operational fires and maneuver. As such, planners must provide for the establishment and sustainment of these networks with the same energy intensity devoted to traditional combat units. Given this central role of sensor networks, a planner needs to provide for sufficient resources to establish and maintain sensor networks during the campaign plan.

There are obvious advantages to a capable, persistent sensor network, which will both hinder the enemy's operational system, and advance the functioning of the friendly system. As situation awareness is gained, operational fires can be used as the attrition element against enemy forces, and facilitate friendly operational maneuver. High quality situation awareness enables efficient, precise networked operations, allowing a campaign to be conducted more effectively, and with less danger of culmination. Given this central role to campaign success, it seems that the current version of FM 3-0 inadequately addresses the need to establish an effective sensor network early in a campaign.[62]

### Situation Awareness Drives Dispersion

Situation awareness allows a force to safely utilize dispersion within a campaign. With network-centric capabilities, dispersed forces are still able to work coherently within in time and space to achieve the system's unifying aim. The resulting framework of battles may be barely recognizable compared to traditional frameworks (using physical lines of operations), but the unifying structure will be there. There will be large pockets of "white space" (areas where no troops are physically deployed), being observed only by the sensor network. Deployment of ground forces will depend on the need to seize bases, seize terrain as part of operational maneuver, and take actions directly against enemy forces when the sensor network is insufficient to the task. Such employment is likely to be characterized by specifically tailored units applied to specific tasks, backed up by joint fires and other "reachback" support.

[62] FM 3-0 contains a significant discussion of information superiority in Chapter 11. The author suggests

### Increased Operational Reach of Forces

Operation Enduring Freedom is the most recent example of air, ground, and naval forces "reaching" from multiple locations. This recent experience suggests that the traditional means of considering operational reach, and the metrics used to calculate operational reach, have changed. Operational reach should now be considered to have at least three facets. Referring back to Chapter 3 of this work, a conventional force has sensor, fires, and physical control dimensions that were often similar. In a network-centric construct these dimensions are different (e. g., the operational reach of force's sensors may be much larger than its ability to physically control terrain).

For the networked force, the increased complexity is that each force has to be considered in the "sensors-fires-physical control" dimensions simultaneously. For example, a ground unit is traditionally considered capable of operational reach depending on its abilities to physically control ground and employ fires. But if it has UAVs, with a 50 mile operational radius, the operational reach of that unit can be considered to be 50 miles (since the UAVs can be used as a conduit to employ supporting fires). A campaign planner has to clearly understand the operational reach of the forces he is planning to use, given this new paradigm.

In a network-centric environment, a unit is particularly valued in terms of its capabilities to augment and support the sensor network. In this sense, joint forces will find themselves providing robust, sustained ISR systems over critical areas (augmented by combat action when needed). The establishment of a "persistent" sensor network expands weapons capabilities out to their maximum ranges, and improves the efficiency with which they are used.[63] In a networked

---

that the employment of sensor networks is central to campaign design.

[63] In the past, for example, a single aircraft would have to fly to a target, take time to locate it, and attack it. Now it can fly to the target, with its target already under observation, and receive updated information along the way. Theoretically, such efficiency will permit more sorties to be flown, with more kills per sortie. Hence, greater operational pressure.

environment, gaining situation awareness translates to the ability to apply lethal force. Hence, the sensor network is an agent of operational reach.

Based on the fundamental campaign analysis, a planner must consider required assets for the campaign. A useful way to address the issue is to consider the employment of force as "pressure" directed against key elements of the enemy system. [64] To apply "pressure" he needs to think in terms of sensors, fires, and physical control. Each of these facets of operational reach serves as a means for operational pressure. Friendly forces must then be employed within operational reach of these areas to build pressure. The campaign then is a framework of pressure points (or "battles" in Naveh's terms), sequentially and simultaneously across time and space, designed to collapse the enemy system (achieve the unifying aim).

Gauging the true operational reach of forces is difficult, as the challenges of physical distance are not erased. It is immensely difficult to coordinate forces from many remote bases and mass them (or their effects) in a certain area. Fuel still gets used up, ammo gets expended, and systems wear out and need maintenance. Operating from dispersed locations increases erosion in this sense. It is still preferable to operate forces from very capable bases, and across short distances. This analysis must adjust the operational reach for these forces considering the theater environment (based on terrain and weather, among other factors).

A networked force requires a complex operational reach calculus. Operational reach is not a single radius of action drawn around a single point. Expanding on Naveh's concept of erosion, the further the physical distance, the endurance of a force is diminished, and the greater the sustainment difficulties. One of the challenges of dispersion in a campaign is that there are potentially accelerated erosive effects on the dispersed assets that are in use. So as a planner structures his operational approach, he needs to consider what effects or results he can expect

[64] James J Schneider, *The Structure of Strategic Revolution*, (Novato, CA: Presidio Press, 1994), 17-25.

from each element of the force, given the physics of the theater and the relevant battlespace. This may require a certain pacing of operations to avoid "burning out" key assets. If the planner is not satisfied with the potential tempo when he "paces" the operation, additional forces (mass) are needed to attain the desired tempo (momentum).

There is some evidence (primarily from Operation Enduring Freedom) suggesting that network-centric forces gain efficiencies from improved logistics, thanks to the information technologies used to support the sustainment system. Such technologies feature logistical systems with improved focus and precision, effectively enhancing efficiency and reducing delivery time for supplies. Precise use of forces reduces demand on support system, which can mean that a higher quality support can be provided to deployed forces. This improved support can help generate increased operational reach of units as well, due to improved availability rates, and by supporting the high operating tempo of units actually engaged in operations.[65]

### Increasing Battlespace of Ground Units

The battlespace of ground forces expands in a networked environment. The increasing availability of sensors and improved ability to generate shared situation awareness allows a dispersed, focused use of ground forces within a unit area of operations (see the "Situation Awareness Drives Dispersion" discussion above). Kosovo and Afghanistan feature focused application of ground forces to accomplish specific tasks in the execution of the campaign. Essentially, increased situation awareness leads to greater efficiency and precision in use of forces (which both counters erosion and magnifies the effect of "mass" to sustain operational momentum). Forces can be used more in terms of what has to be achieved, and less in terms of guarding against the unknown. This can potentially led to the ability to accomplish tasks with fewer forces, to the degree we feel secure against surprise actions by the opponent.

[65] Smith, "Network-Centric Warfare: What's the Point?" 60-63.

Newer formations, such as Force XXI and Interim Brigades, have improved ISR assets, which permit them to build situation awareness out to extended ranges (and results in increased operational reach in the "sensors" and "fires" aspect). This increased operational reach for ground combat formations opens new opportunities for operational manevuer. Ground formations maneuvered into the depth of an enemy's operational system can potentially have increased, perhaps devastating impact. A planner must consider the wide discrepancies between the battlespace of a traditional, non-networked unit, and a networked unit. A planner needs to correctly assess the value of this expanded battlespace, and properly exploit this capability within a campaign.

### Dispersion vs. Mass

Situation awareness enables a commander to employ highly dispersed ground forces, and retain the ability to mass all forms of combat power. Operations in Afghanistan show that phenomenal amounts of fires can be concentrated in coordination with ground forces. Yet the calculus a planner must use to balance dispersion vice mass to sustain an operation remains highly complex. Recall that mass performs two functions, which are to secure favorable tactical battle outcomes, and to sustain operational momentum. The amount of mass required operationally depends on at least three variables.

The first variable in this equation is the level of situation awareness. When situation awareness is low, the enemy's disposition and intent is unclear, and friendly forces must counter against uncertainty with reserves, security forces and physical control of vast areas of terrain (in order to ensure that the enemy is "not there"). Consider Operation Desert Storm where the low levels of situation awareness led to specific formations assigned to security missions, others assigned to gain situation awareness, and a general disposition of forces to protect against the

unknown. Essentially, if there is little situation awareness, then traditional means of force employment are required.

The second consideration is the degree to which the enemy has been able to mass his forces. If the enemy can achieve mass, then friendly forces must counter with mass. This is a rather simplistic "mass requires mass" principle, but it is essential to frustrate the enemy operational system. Interestingly enough, both Operation Desert Storm and Operation Enduring Freedom contain situations where enemy forces were able to mass physically, despite operational fires. These concentrations had to be overcome by opposing mass (in the form of concentrated effects, and physical concentration of forces on the ground).

A third variable is the need for "presence", normally as part of a peacekeeping operation. When peacekeeping operations are needed, sensor networks cannot realistically demonstrate presence, and employment of forces has to be based on presence (showing everyone that we are around anywhere all the time). A highly dispersed unit has extreme difficulty demonstrating "presence" to a population. If the mission is to actually control events within a given area, then ground forces are likely to be needed in larger numbers. A large civilian population requires a large number of peacekeepers to achieve the desired results.

Fundamentally, the planner must be satisfied that he has sufficiently provided for mass (a holistic combination of forces, fires, and non-lethal effects) to sustain operational momentum. This satisfaction must stem from an assessment of the level of situation awareness that will be achieved, the ability of his forces to concentrate from their dispersed locations, and a similar assessment regarding the enemy's ability to mass.

### Long-Range Planning in a Real-Time Environment

Network-Centric Warfare offers a special challenge to the campaign planner, which is already manifested in current operations. Near real time information impacts at multiple echelons

simultaneously. This situation demands a combination of a traditional campaign design with a network-centric design. A planner usually plans for the mid-term to long-term, yet information continually arrives which informs and updates the plan. A given campaign design will receive continual updates, yet must still be the long-term vision guiding the campaign. A planner must oversee this blending of strategic, operational, tactical levels without allowing operations to spin out of control as tactical commanders try to chase short-term tactical advantages. A planner must maintain Naveh's cognitive tension in a near-real time environment.

## Implications Regards Operational Maneuver

The fourth criterion asks if Network-Centric Warfare has changed the nature of operational maneuver within a campaign? FM 3-0 defines maneuver as the employment of forces, through movement combined with fires, to achieve a position of advantage relative to the enemy. Operational maneuver involves placing forces and resources at the critical place in time to achieve an operational advantage. It involves creating favorable conditions for tactical battles within a campaign.[66]

Applying these definitions to the historical operations reviewed above suggests that operational maneuver has gained a new level of complexity. The transition of entities, attributes, and relationships within a networked force creates a force with multifaceted operational reach and increased dispersion. This new operational system provides at least three potential interpretations of "positional advantage. Operational maneuver, in its holistic sense, is a blend of positional advantage that pertains equally to sensor capabilities, fires, and physical control of ground.

Sensor networks now play a role within operational maneuver. As noted above, there is a significant advantage gained by establishing a robust sensor network against the enemy operational system. Establishing such a network helps hinder or shock the enemy's operational

[66] FM 3-0, 4-4.

systems (by attacking the systems, or simply negating them through counter actions). Positional advantage involves positioning the sensor network in such a way to support favorable tactical outcomes, and to sustain operational momentum.

A similar challenge exists for fires. The correct mix of forces has to be put in place to provide the necessary fires to hinder the enemy's operational systems. Positional advantage in this case is placing forces in locations from which they can generate enough combat power over time to cause the desired damage to the enemy's operational system. Generally, the "right time & place" will change often across the time and space of the campaign.

Positional advantage regarding physical control of key terrain is perhaps the simplest to comprehend (ground forces in control of areas that enable other aspects of the campaign, or hinder enemy operational system). Given the dispersed nature of Network-Centric Warfare, instances of physical control of terrain can be limited. However, the necessity for physical control of terrain depends greatly on campaign aims, and on the nature of interaction between enemy and friendly operational systems (see the dispersion vs. mass discussion above).

As mentioned earlier, the enemy operational system will be at least as adaptive as the US operational system. The enemy will recognize the strengths of the US system, and work to counteract or evade its efforts. This competition of two complex adaptive systems, both of which are adapting as quickly as possible to each other and to a changing environment, places a premium on the effective employment of operational maneuver. Positional advantage is required to truly frustrate the enemy system and its attempts to adapt. The campaign planner will need to utilize a careful combination of maneuver across all three of these facets to succeed (e.g. the campaign is structured to achieve positional advantage in terms of physical control of terrain, which enables positional advantage in terms of sensors and fires).

In summation, Network-Centric Warfare has changed the nature of operational maneuver.

There is a need to consider positional advantage in terms of sensors, fires, and maneuver forces to win the tactical battles and sustain operational momentum. This new complexity has created more options for conducting operational maneuver and attaining desired aims. Sensor networks are a key prerequisite for effective functioning of a networked force. Therefore, the employment of such networks is now a key feature of maneuver. For the joint force, operational maneuver is a blend of positional advantage that pertains equally to sensor capabilities, fires, and physical control of terrain. Sensor networks are a key element of operational maneuver.

## Network Centric Campaign Planning

What then, does a network-centric campaign look like? This section is intended to integrate the conceptual campaign described in Chapter 3 with the results of the analysis in later chapters. Therefore, what follows is a brief description of planning for a primarily network-centric campaign.

A campaign planner recognizes that the tremendous capabilities of a networked force depend squarely on the early deployment and sustainment of a sensor network. Although some sensor assets will already available (from national resources and existing theater forces), the planner must quickly address immediate information and situation awareness requirements. As situation awareness is gained, actions can be taken to mature the campaign plan, facilitate initial operational maneuver, and conduct actions (information operations, operational fires, etc.) to hinder the enemy's operational system (See Step 1 in Figure 3 below).

The next stage of the campaign is designed to exert "pressure" against key elements of the enemy operational system. This pressure is developed across the three facets of operational reach discussed above (sensors, fires, and physical control). Perhaps the biggest challenge facing the planner is how to apply limited available assets in order to generate desired operational pressure. A highly dispersed joint force can apply a little bit of pressure everywhere, or a whole

lot of pressure somewhere. Operational maneuver within this campaign melds these three aspects of operational pressure, at all appropriate decisive points. The campaign then is a series of pressure points, sequentially or simultaneously across time and space, designed to collapse the enemy system (See Step 2 in Figure 3 below).

The campaign quickly gains a cyclic "sensor network extension – operational maneuver-sensor network extension" pattern. Because situation awareness is so central to network-centric operations, planners must continually provide for the establishment and sustainment of a sensor network as a precondition for operational maneuver. Operational maneuver not only gains positional advantage physically, relative to the enemy operational system, but also creates conditions for sensor networks to gain the required level of situation awareness for future operations (e. g. attacking air defense systems or counter-reconnaissance forces). Sensor networks must be maneuvered with the same energy and intensity traditionally devoted to the maneuver of "combat units."[67] Operational design must include employment and maneuver of the sensor network as a primary enabler of any campaign phase (See Step 3 in Figure 3 below).

A campaign planner should expect that elements of the enemy operational system are indiscernible, due to concealment, enemy adaptiveness, or lack of sensor capability. As mentioned in Chapter Three, the question is which elements of the enemy systems are detectable and susceptible to attack. When the sensor network is limited or insufficient, a network-centric force must maneuver forces to gain observation of the enemy system, or must establish physical control of geographic areas to prevent functioning of the enemy system. The force structure employed depends on which of these facets is required to achieve the desired pressure (See Step 4 in Figure 3 below).

[67] Although this idea is partially expressed in FM 3-0, the monograph author contends that this idea is central to a campaign, even with today's partially networked force, and should therefore be considered a key element of operational design and operational maneuver. See HQDA, *FM 3-0*, 11-2 to 11-3.

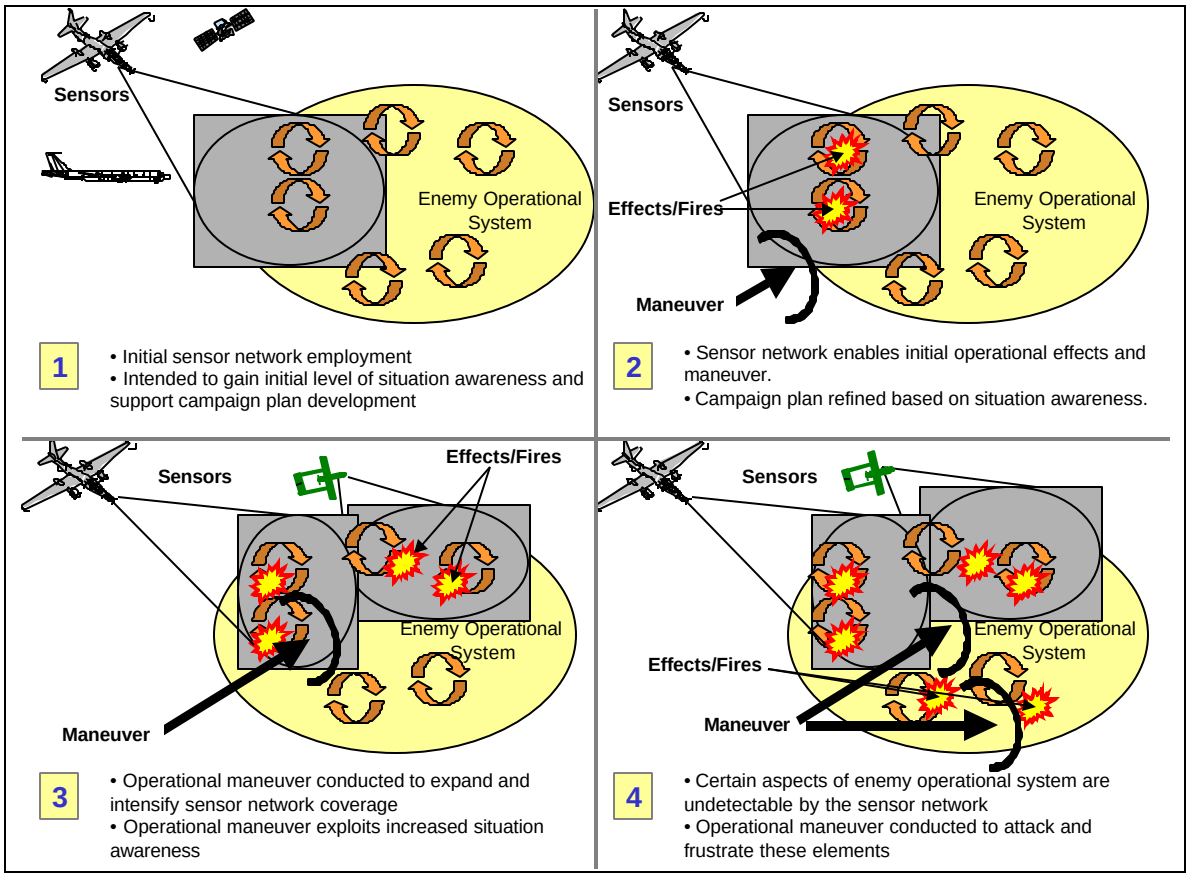


**Figure 3. Network-Centric Campaign Design**

Finally, a network centric campaign carefully considers the erosive effects of the enemy force and the theater itself (time and space factors). The campaign allows for sufficient forces to counteract these erosive effects, concurrently frustrating the enemy's "mass," and maintaining operational momentum toward friendly campaign objectives. Hence, a campaign plan must contain the right balance of networked and traditional means to attain operational objectives. A campaign planner must correctly identify this balance, and employ forces correctly as part of operational maneuver against the enemy's operational system.

## Implications for Operational Design

This analysis reinforces the existing concepts of centers of gravity, decisive points and objectives regarding properly analyzing and structuring a campaign. A planner must still accurately assess the enemy's operational system, to include his centers of gravity, critical

requirements, and critical vulnerabilities. Without this sound basis to the campaign, technological advancement will not in and of itself produce a winning campaign.

> Operational planning doctrinally focuses on determination of the desired end-state and identification of the enemy's center of gravity and critical vulnerabilities at each of the levels of war. Doctrine also tells us that planning must additionally include analysis of the *enemy's* desired end-state and *our own* centers of gravity and critical vulnerabilities. Expediency has no place in the equation.[68]

Hence, the planner must correctly assess the enemy's operational system (discerning its centers of gravity and vulnerabilities), and identify decisive points and objectives relative to its defeat. Beyond this fundamental basis for campaign planning, Network-Centric Warfare significantly impacts the other elements of operational design.

A network-centric campaign profoundly alters the idea of lines of operations. Essentially, a network-centric force can mass combat power nearly anywhere within its area of operations on short notice. Given the general dispersion of forces, and the likely continual shifting of assets throughout the theater, a geographic "line" of operations may be difficult to discern. A line of operation may actually look like an amorphous, 3-dimensional area, which is continually changing. Within this area, an observer will see the massing of effects and/or forces for short periods of time at geographically disparate locations in time and space. The line of operation, if it exists, will be more of the logical type discussed in FM 3-0. A campaign will link these disparate actions in a certain sequence to achieve a campaign aim. Of course, in situations requiring significant massing of forces, logistics will emerge as an overriding consideration, and the existence of lines of operations related to lines of communications are likely to emerge.

The current ideas of operational reach and operational approach are insufficiently developed to be useful for a network-centric force. Although the existing definition correctly defines operational reach as dependent on sustainment, bases, and weapons ranges, more is needed.

---

[68] Vincent J. Goulding, Jr., "From Chancellorsville to Kosovo, Forgetting the Art of War", *Parameters*, Vol. XXX, No 2. Summer 2000, 9.

These elements must be expanded to address the new complexity of the sensor-fires-physical control dimensions of operational reach and approach.

The idea of a culminating point takes on special meaning as well. A network-centric force could potentially culminate in each of the three facets of operational reach discussed above. There may be insufficient sensor capability to generate the needed pressure on enemy systems. Or, there may be insufficient effects/fires delivery means available. Or insufficient ground maneuver assets to affect physical control. Operational design must consider the operational reach of forces in each of these areas, and structure the campaign to avoid culmination.

A network-centric campaign is likely to employ simultaneous and sequential operations. Given the efficiencies provided by increased collaboration and communication, a higher occurrence of simultaneous operations is possible. Although the preference is for simultaneous operations (to maintain a high tempo), circumstances are likely to compel some degree of sequential operations. In a similar fashion, network-centric campaigns are highly disposed to non-linear operations, but linear operations may be used when situation awareness levels are low (thus requiring an extensive, contiguous deployment of ground forces to achieve desired aims).

As a final point, the current set of design elements fails to address the importance of establishing a sensor network early in the campaign. The elements of operational design are specifically used to assist the commander (and his planners) in visualizing the campaign he intends to undertake. The current list of elements does not directly lead the commander to address the central importance of a sensor network to his campaign. Nor do they help him to visualize the need to conduct operational maneuver, which now includes sensor networks, as well as the traditional aspects of fires, and physical control of terrain. There is a clear need to recognize the employment of sensor networks as a key element of operational design.

## Conclusion

It is appropriate to revisit the monograph's delimitation before concluding. This assessment emphasizes the role of ground forces within a "network-centric" campaign design, and there are presuppositions that the political will exists to use ground forces, and campaign objectives cannot be achieved without ground forces. Furthermore, the author did not fully address the challenges of coalition warfare, or the challenges of conducting a campaign with legacy and transformation forces. The assessment focuses on campaigns against organized military forces, pursuing their own campaign objectives in an "operational" fashion.

Network-Centric Warfare is here now, and is already embedded in how we conduct joint operations, thanks to sustained investments in communications, information, sensor, and weapon technologies. A partial implementation of Network-Centric Warfare has been achieved. Commanders and planners need to realize that they are dealing with a partially network-centric joint force today. Since modernization and transformation are continuing daily, the potential impacts on for operational design are growing.

A planner has to realize that Network-Centric Warfare is changing the operational system that he will employ. The forces he is working with are gaining improved operational reach, are very efficient in terms of generating combat power, and can be employed more precisely than in the past. He must consider the key elements of sensor networks, linked fires, and physical occupation/domination of terrain. Above all, he needs to realize that he still has to use operational art. Network-Centric Warfare is pointless unless the planner properly analyzes the operational systems of both sides. Given a proper analysis, the campaign planner must clearly design a campaign that properly focuses his sensor networks, operational fires, and maneuver forces to disable the enemy operational system.

Network-Centric Warfare has changed the nature of operational maneuver. Sensor networks

are a key prerequisite for effective functioning of a networked force. Therefore, the employment of such networks is now a key feature of maneuver. For the joint force, operational maneuver is a blend of positional advantage that pertains equally to sensor capabilities, fires, and physical control of terrain. Sensor networks are a key element of operational maneuver.

Network-Centric Warfare directly impacts the operational design of a campaign. The operational design elements identified in FM 3-0 are dramatically affected. Operational reach has reached new levels of complexity. The use of highly dispersed and precise operations applies a new interpretation to the term "lines of operations," which may defy the current description of "physical or logical. Beyond the implications for these elements, there is a clear need to recognize the employment of sensor networks as a key element of operational design.

There are many implications here for the US Army. Initiatives to further network forces need to be pursued (particularly to facilitate joint operations). Doctrinal changes are needed, both to recognize the existence of networked joint forces, and to incorporate the essential functioning of Army units within this force. The dispersed and precise nature of network-centric operations suggests that lower echelon Army units (brigade and battalion) must be very capable of networking and operating within a joint force. These units must be prepared to act independently, self-synchronizing with other remote units as part of the larger scheme of operations. In terms of force design, formations need to be fielded which can fully exploit network-centric concepts (in terms of sensors, fires, and control of terrain). But force designers must also recognize that ground maneuver formations still need to destroy enemy "mass" when it occurs. Therefore, US Army formations need a structure that permits full exploitation of network-centric concepts, allows mastery of close combat, and provides for operational durability.

Network-Centric Warfare is working profound changes across the armed forces. Although much of these changes are related to technological advances, we need to remain cognizant of the other factors that Michael Handel identifies as contributing to victory:

> In modern history no major conflict has ever been won by technologically superior weapons alone, and in those wars where qualitative superiority has appeared to be the deciding factor, the conflicts have been short and the qualitative assets of the victor have been other than technological: superior military organization, staff work, planning, and political leadership, as well as training and morale.[69]

In this quote lies the real promise of Network-Centric Warfare. It is more than "a technologically superior weapon." Instead, Network-Centric Warfare is very much about superior military organization, highly informed staff work, superior planning, and leadership. By improving the relationships within a complex operational system, it promises to yield a decisive advantage.

[69] David C. Evans, Mark R. Peattie, *Kaigun: Strategy, Tactics, and Technology in the Imperial Japanese Navy 1887-1941*, (Annapolis, Maryland: Naval Institute Press, 1997), 513. Citing Michael Handel. "Numbers do Count: The question of Quality vs. Quantity:. *Journal of Strategic Studies* 4 (September 1981).

# Bibliography


GOVERNMENT PUBLICATIONS

Chairman of the Joint Chiefs of Staff. *Joint Vision 2010*. Washington, D. C. June 1996.

_____. *Joint Vision 2020*. Washington, DC: Government Printing Office, May 2000.

Cohen, William S. and Henry H. Shelton. *"Joint Statement on the Kosovo After Action Review."* 14 October 1999, prepared joint statement presented by the Secretary of Defense and the Chairman of the Joint Chiefs of Staff before the Senate Armed Services Committee.

Department of Defense. Assistant Secretary of Defense for Command, Control, Communications, & Intelligence. *Network Centric Warfare. Department of Defense Report to Congress, 27 July 2001*. Available at http://www.c3i.osd.mil/Network-Centric Warfare/.

Joint Chiefs of Staff. *Joint Publication 1: Joint Warfare of the Armed Forces of the United States*. Washington, D. C. Joint Electronic Library (CD-ROM), 10 January 1995.

_____. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*. Washington, D. C. 12 April 2001, amended 23 January 2002. Available at http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf. Last visited 19 April 2002.

_____. Joint Publication 3-0: Doctrine for Joint Operations. Washington, D. C. Joint Electronic Library (CD-ROM), 1 February 1995.

_____. Joint Publication 3-33: Joint Force Capabilities. Washington, D. C. Joint Electronic Library (CD-ROM), 13 October 1999.

Headquarters, United States Army Training and Doctrine Command. *Operational and Organizational (O&O) Concept for the Army XXI Division-level Heavy Force, Including the Brigade Combat Team and the Cavalry Squadron (Coordinating Draft),* Fort Monroe, VA, December 1999.

_____. *The Brigade Combat Team Organizational and Operational Concept, Final Version, 30 June 2000*. Fort Monroe, VA, 2000.

_____. *The Objective Force Maneuver Unit of Action: The Foundations of Army Transformation and the Objective Force Concept (draft), 17 January 2001*. Fort Monroe, VA, 2001.

_____. *The Objective Force Maneuver Unit of Action: The FCS Combat Battalion Operational and Organizational Concept (draft), 15 Feb 2001*. Fort Monroe, VA, 2001.

_____. *Division Capstone Exercise Phase I (DCX I) Initial Insights Memorandum (IIM),* April 2001. Fort Monroe, VA, 2001.

Office of the Secretary of Defense. *Unmanned Aerial Vehicle (UAV) Roadmap,* Washington, D. C., 6 April 2001.

The Joint Staff, C4 Systems Directorate, Information Superiority Division (J6Q), *Enabling the Joint Vision*, Washington, D. C., May 2000. Available at http://www.dtic.mil/jcs/j6/enablingjv.pdf. Site last visited 20 March 2002.

TRADOC Analysis Center, *TRADOC Combined Arms Reconnaissance Study Phase I Final Report, (TRAC-TR-0900),* Fort Leavenworth, Kansas, 31 August 2000.

_____. *TRADOC Combined Arms Reconnaissance Study Phase II (TRAC-L-TR-01-005),* Fort Leavenworth, Kansas, 15 December 2000.

_____. *Initial Insights Memorandum (IIM) for the Division Capstone Exercise Phase II (DCXII), TRAC-F-TR-02-004,* Fort Leavenworth, Kansas, October 2001.

_____. *Final Report for the Division Capstone Exercise (DCX*), *TRAC-F-TR-02-006,* Fort Leavenworth, Kansas, March 2002.

U. S. Department of the Army. *FM 3-0: Operations*. Washington, D. C., June 2001.

_____. *FM101-5-1: Operational Terms and Graphics*. Washington, D. C., 1997.

BOOKS

Alberts, David S., John J. Garstka, Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority, 2d Edition Revised*. Washington, DC: CCRP Publications, 2000.

Alberts, David S., John J. Garstka, Richard E. Hayes, David A. Signori, *Understanding Information Age Warfare*. Washington, DC: CCRP Publications, 2001.

Blackwell, James. *Thunder in the Desert*. New York: Bantam Books, 1991.

Clark, Wesley K. *Waging Modern War: Bosnia, Kosovo, and the Future of Combat.* New York: Public Affairs, 2001.

Daalder, Ivo and Michael O'Hanlon. *Winning Ugly: NATO's War to Save Kosovo*. Washington, D. C.: Brookings Institution, 2000.

Evans, David C. and Mark R. Peattie. *Kaigun: Strategy, Tactics, and Technology in the Imperial Japanese Navy 1887-1941*. Annapolis, Maryland: Naval Institute Press, 1997.

Gordon, Michael R. and Bernard E. Trainor. *The General's War: The Inside Story of the Conflict in the Gulf.* New York: Little, Brown, and Co., 1995.

Ignatieff, Michael. *Virtual War: Kosovo and Beyond*. New York: Metropolitan Books, Henry Holt and Co., 2000.

Lambeth, Benjamin S. *NATO'S Air War for Kosovo: A Strategic and Operational Assessment*. Santa Monica: Rand, 2001.

Leonhard, Robert R. *Fighting By Minutes: Time and the Art of War*. Westport, CT: Praeger Publishers, 1994.

_____. *The Principles of War for the Information Age*. Novato, CA: Presidio Press, 1998.

Naveh, Shimon. *In pursuit of Military Excellence: The Evolution of Operational Theory*. Portland, OR: Frank Cass Publishers, 1997.

O'Hanlon, Michael. *Technological Change and the Future of Warfare*. Washington: Brookings Institution Press, 2000.

Owen, Robert C. *Deliberate Force: A Case Study in Effective Air Campaigning*. Maxwell AFB: Air University Press, 2000.

Scales, Robert H., Jr. *Future Warfare: Anthology*. Carlisle Barracks, PA: U. S. Army War College, 2000.

Schneider, James J., *The Structure of Strategic Revolution*. Novato, CA: Presidio Press, 1994.

Swain, Richard M. *"Lucky War": Third Army in Desert Storm.* Fort Leavenworth, KS: U. S. Army Command and General Staff College Press, 1994.

U. S. News and World Report. *Triumph without Victory*. New York: Random House, 1992.

Watts, Barry D. *Clausewitzian Friction and Future War*. Washington, D.C.: National Defense University Press, 1996.

ARTICLES

Biddle, Stephen, Wade P. Hinkle, and Michael P. Fischerkeller. "Skill and Technology in Modern War." *Joint Forces Quarterly* (Summer 1999): 18-27.

Burger, Kim and Andrew Koch. "Afghanistan: The Key Lessons" *Jane's Defence Weekly*, (January 2, 2002).

Cebrowski, Arthur K., and John J. Garstka. "Network-Centric Warfare: Its Origin and Future." *Proceedings* (January 1998). 1997. Available online at http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm . Site last visited 20 March 2002.

Crock, Stan. "Cooperation: A Key to Victory in Afghanistan." *Business Week Online*

(December 17, 2001). Available at http://www.businessweek.com/bwdaily/dnflash/dec2001/nf20011217_5178.htm. Site last visited 20 March 2002.

Deptula, David A. "Embracing Change: US Air Force Transformation Will Expand the Nation's Strategic Options." *Armed Forces Journal International* (October 2001): 69-71.

Diamond, John. "Pentagon Plumbs Lessons From the War", *Chicago Tribune.* (January 14, 2002).

Fulghum, David A. "Navy Exploits P-3 in Overland Recce Role." *Aviation Week & Space Technology* (March 4, 2002).

_____. "Intel Emerging as Key Weapon in Afghanistan." *Aviation Week & Space Technology* (March 11, 2002).

Goure, Daniel. "The Army's Policy Nettle." *Armed Forces Journal International* (October 2001): 44-54.

Goulding, Vincent J., Jr. "From Chancellorsville to Kosovo, Forgetting the Art of War." *Parameters* Vol XXX, No 2. (Summer 2000): 4-18.

Grossman, Elaine M. "Air Force Chief Launches Major Effort to Improve Targeting." *Inside the Pentagon (*November 8, 2001).

Haven, Paul. "Operation Anaconda under Scrutiny." *Newsday.com (*March 18th, 2002). Available from http://www.newsday.com/. Site last visited 18 March 2002.

Innocenti, Charles W. "Applying the Unmanned Aerial Vehicle (UAV) to Brigade Reconnaissance and Surveillance (R&S) Operations." *CTC Quarterly Bulletin*, 1st QTR, FY00, No. 00-4, (MAR OO): 36-42.

Lasswell, James. "Waterborne Warriors: Putting The Amphibious Pieces Together." *Armed Forces Journal International* (January 2001): 36-41.

Loeb, Vernon and Thomas E. Ricks., "1's and 0's Replacing Bullets in U. S. Arsenal.", *Washington Post* (February 2, 2002).

McConnell. Kirk and Mike Meermans. "Nowhere to Hide" *Armed Forces Journal International* (July 2001): 46-50.

Murdock, Paul. "Principles of War on the Network Centric Battlefield: Mass and Economy of Force." *Parameters* Vol. XXXII, No 1. (Spring 2002): 86-95

Murray, William S. "A Will to Measure," *Parameters* Vol. XXXI, no. 3 (Autumn 2001): 134-147.

Redd, Scott. "Sustained Assured Access: The Navy's Role in Joint Warfare" *Armed Forces Journal International* (September 2001): 66-70.

Ricks, Thomas E. and Bradley Graham. “Surprises, Adjustments, and Milestones for U. S. Military.” *Washington Post* (March 10, 2002).

Roos, John G. “An All-Encompassing Grid.” *Armed Forces Journal International* (January 2001): 26-35.

Scales, Robert L. “Checkmate by Operational Maneuver.” *Armed Forces Journal International* (October 2001): 38-42.

Singer, Jeremy and Frank Tiboni, “New Intel Devices Get Trial By Fire in Afghanistan,” *Defense News*, (March 25-31, 2002).

Smith, Edward A., Jr. “Network-Centric Warfare: What’s the Point?” *Naval War College Review* (Winter 2001).

Tiboni, Frank. “Instantaneous Attack Capability near for U. S.” *Defense News* (January 7-13, 2001).

MONOGRAPHS

Jones, Christopher A. "Unmanned Aerial Vehicles (UAVs): An Assessment of Historical Operations and Future Possibilities". Research Paper, Air Command and Staff College, March 1997.

OTHER REFERENCES:

Borque, Stephen A. “Desert Saber: The VII Corps in the Gulf War” Ph. D. diss., Georgia State University, 1996.

Conetta, Carl. "Disengaged Warfare: Should we make a virtue of the Kosovo way of war?" *Project on Defense Alternatives Briefing Memo 21*, Cambridge, MA: Commonwealth Institute, May 2001. Available at: http://www.comw.org/pda/0105bm21.html. Site last visited 20 March 2002.

Headquarters, United States Army Training and Doctrine Command. *The Objective Force Maneuver Unit of Action Concept Briefing.* Fort Monroe, VA, 24 January 2001.